(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102007726 B
(45)授权公告日 2014.05.14

(21)申请号 200980113336.6
(22)申请日 2009.04.24
(30)优先权数据
2008-113530 2008.04.24 JP
(85)PCT国际申请进入国家阶段日
2010.10.15
(86)PCT国际申请的申请数据
PCT/JP2009/001903 2009.04.24
(87)PCT国际申请的公布数据
WO2009/130917 JA 2009.10.29
(73)专利权人 富士通株式会社
地址 日本神奈川县
(72)发明人 岩尾忠重 增渊健太郎 中嶋千明 池本健太郎 古贺俊介 高桥勇治
(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 李伟 陈桂兰
(51)Int.Cl.
H04L 9/08(2006.01)
(56)对比文件
CN 1674496 A,2005.09.28, 全文.
US 2002037736 A1,2002.03.28, 全文.
JP 2007104310 A,2007.04.19, 全文.
CN 101110831 A,2008.01.23, 全文.
审查员 池芳

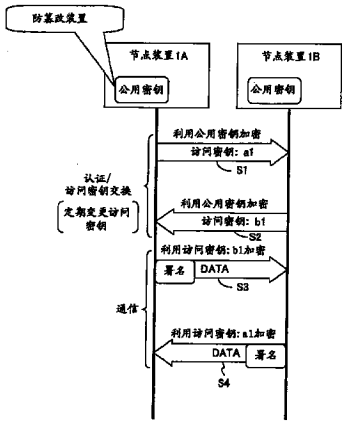
权利要求书3页 说明书27页 附图18页

(54)发明名称

节点装置以及程序

(57)摘要

在由多个节点装置构成的网络中的第1节点装置中,访问密钥生成部每隔第1时间变更第1节点装置所固有的加密密钥、即第1访问密钥。公用密钥生成部每隔第2时间变更在多个节点装置中公用的公用密钥。第1节点装置使用所生成的公用密钥对所生成的第1访问密钥进行加密并发送,并且接收由第2节点装置发送来的、包含使用公用密钥对第2节点装置的第2访问密钥进行加密得到的数据的访问密钥通知帧。解密部通过使用所生成的公用密钥对接收到的访问密钥通知帧进行解密来取得第2访问密钥。发送部发送使用第2访问密钥对明文帧进行加密得到的加密帧,该明文帧附加有使用公用密钥对包含根据明文帧计算出的散列值的数据进行加密得到的署名数据。



CN 102007726 B

1. 一种节点装置，其特征在于，

是由包含第 1 节点装置和第 2 节点装置的多个节点装置构成的网络中的上述第 1 节点装置，具有：

访问密钥生成部，每隔第 1 时间变更生成上述第 1 节点装置所固有的加密密钥、即第 1 访问密钥；

公用密钥生成部，每隔在上述多个节点装置中共同的时间、即第 2 时间变更生成在上述网络内的上述多个节点装置中公用的公用密钥；

访问密钥通知部，使用所生成的上述公用密钥对所生成的上述第 1 访问密钥进行加密并向上述第 2 节点装置发送；

访问密钥接收部，接收从上述第 2 节点装置发送来的包含访问密钥通知数据的访问密钥通知帧，该访问密钥通知数据是使用上述公用密钥对上述第 2 节点装置所固有的加密密钥、即第 2 访问密钥进行加密得到的数据；

访问密钥解密部，使用所生成的上述公用密钥对上述访问密钥通知数据解密，由此根据上述访问密钥通知数据取得上述第 2 访问密钥；

数据发送部，向第 1 明文帧附加使用上述公用密钥对包含根据该第 1 明文帧计算出的第 1 散列值的数据进行加密得到的第 1 署名数据，使用通过解密得到的上述第 2 访问密钥对附加有上述第 1 署名数据的上述第 1 明文帧进行加密并作为第 1 加密帧发送；

数据接收部，从上述第 2 节点装置接收利用上述第 1 访问密钥对第 2 明文帧进行加密得到的第 2 加密帧，该第 2 明文帧附加有使用上述公用密钥对包含第 2 散列值的数据进行加密得到的第 2 署名数据，其中，所述第 2 散列值是根据上述第 2 明文帧计算出的；

数据解密部，使用上述第 1 访问密钥对上述第 2 加密帧进行解密，从而根据上述第 2 加密帧得到附加有上述第 2 署名数据的上述第 2 明文帧；和

一致性确认部，通过使用所生成的上述公用密钥对上述第 2 署名数据解密来取得上述第 2 散列值，根据上述第 2 明文帧计算第 3 散列值，并确认是否取得了上述第 2 散列值和上述第 3 散列值的一致性。

2. 根据权利要求 1 所述的节点装置，其特征在于，

上述数据发送部使上述第 1 明文帧中包含用于唯一识别上述第 1 明文帧的第 1 识别符和表示第 1 发送时刻的信息；

在上述数据解密部从上述第 2 加密帧解密得到的上述第 2 明文帧中包含的第 2 识别符与从过去接收过的第 3 加密帧解密得到的第 3 明文帧中包含的第 3 识别符相等的情况下，上述一致性确认部还废弃上述第 2 明文帧和上述第 3 明文帧中的通过解密得到的信息表示较新的发送时刻的一方。

3. 根据权利要求 2 所述的节点装置，其特征在于，

具有：

时刻同步帧发送部，生成第 1 时刻同步帧作为时刻同步帧并发送，上述第 1 时刻同步帧包含表示上述第 1 节点装置的第 1 当前时刻和上述第 1 节点装置的时刻校准所依据的第 1 同步时刻的数据；

时刻同步帧接收部，从上述第 2 节点装置接收第 2 时刻同步帧，上述第 2 时刻同步帧包含表示上述第 2 节点装置的第 2 当前时刻和上述第 2 节点装置的时刻校准所依据的第 2 同

步时刻的数据；

时刻更新部，比较根据上述第 2 时刻同步帧得到的第 2 同步时刻和上述第 1 节点装置存储的上述第 1 同步时刻，如果上述第 2 同步时刻较新，则将上述第 2 当前时刻设定为上述第 1 节点装置的当前时刻来更新上述第 1 节点装置的时刻；和

存储部，存储上述第 2 同步时刻作为新的第 1 同步时刻，上述新的第 1 同步时刻是上述时刻更新部更新上述第 1 节点装置的时刻而进行的上述时刻校准所依据的；

上述公用密钥生成部根据上述时刻更新部进行了更新的时刻对上述第 2 时间进行计时。

4. 一种第 1 节点装置执行的方法，是由包含第 1 节点装置和第 2 节点装置的多个节点装置构成的网络中的上述第 1 节点装置执行的方法：

每隔第 1 时间变更生成上述第 1 节点装置所固有的加密密钥、即第 1 访问密钥；

每隔在上述多个节点装置中共同的时间、即第 2 时间变更生成在上述网络内的上述多个节点装置中公用的公用密钥；

使用所生成的上述公用密钥对所生成的上述第 1 访问密钥进行加密并向上述第 2 节点装置发送；

接收从上述第 2 节点装置发送来的包含访问密钥通知数据的访问密钥通知帧，该访问密钥通知数据是使用上述公用密钥对上述第 2 节点装置所固有的加密密钥、即第 2 访问密钥进行加密得到的数据；

使用所生成的上述公用密钥对上述访问密钥通知数据解密，由此根据上述访问密钥通知数据取得上述第 2 访问密钥；

向第 1 明文帧附加使用上述公用密钥对包含根据该第 1 明文帧计算出的第 1 散列值的数据进行加密得到的第 1 署名数据，使用通过解密得到的上述第 2 访问密钥对附加有上述第 1 署名数据的上述第 1 明文帧进行加密并作为第 1 加密帧发送；

从上述第 2 节点装置接收利用上述第 1 访问密钥对第 2 明文帧进行加密得到的第 2 加密帧，该第 2 明文帧附加有使用上述公用密钥对包含第 2 散列值的数据进行加密得到的第 2 署名数据，其中，所述第 2 散列值是根据上述第 2 明文帧计算出的；

使用上述第 1 访问密钥对上述第 2 加密帧进行解密，从而根据上述第 2 加密帧得到附加有上述第 2 署名数据的上述第 2 明文帧；

通过使用所生成的上述公用密钥对上述第 2 署名数据解密来取得上述第 2 散列值，根据上述第 2 明文帧计算第 3 散列值，并确认是否取得了上述第 2 散列值和上述第 3 散列值的一致性。

5. 根据权利要求 4 所述的第 1 节点装置执行的方法，

上述作为第 1 加密帧发送的处理是，使上述第 1 明文帧中包含用于唯一识别上述第 1 明文帧的第 1 识别符和表示第 1 发送时刻的信息来进行处理；

确认是否取得了上述第 2 散列值和上述第 3 散列值的一致性的处理是，进一步，在从上述第 2 加密帧解密得到的上述第 2 明文帧中包含的第 2 识别符与从过去接收过的第 3 加密帧解密得到的第 3 明文帧中包含的第 3 识别符相等的情况下，废弃上述第 2 明文帧和上述第 3 明文帧中的通过解密得到的信息表示较新的发送时刻的一方。

6. 根据权利要求 5 所述的第 1 节点装置执行的方法，

生成第 1 时刻同步帧作为时刻同步帧并发送，上述第 1 时刻同步帧包含表示上述第 1 节点装置的第 1 当前时刻和上述第 1 节点装置的时刻校准所依据的第 1 同步时刻的数据；

从上述第 2 节点装置接收第 2 时刻同步帧，上述第 2 时刻同步帧包含表示上述第 2 节点装置的第 2 当前时刻和上述第 2 节点装置的时刻校准所依据的第 2 同步时刻的数据；

比较根据上述第 2 时刻同步帧得到的第 2 同步时刻和上述第 1 节点装置存储的上述第 1 同步时刻，如果上述第 2 同步时刻较新，则将上述第 2 当前时刻设定为上述第 1 节点装置的当前时刻来更新上述第 1 节点装置的时刻；

在存储部中存储上述第 2 同步时刻作为新的第 1 同步时刻，上述新的第 1 同步时刻是更新上述第 1 节点装置的时刻而进行的上述时刻校准所依据的；

上述生成公用密钥的处理，根据上述更新后的时刻对上述第 2 时间进行计时。

节点装置以及程序

技术领域

[0001] 本发明涉及自律分散型网络中的用于安全维护的装置以及程序。

背景技术

[0002] 作为安全性对策的一种，一直在对发送数据进行加密。作为加密的方法，例如有公用密钥方式（也叫做对称密钥加密方式）。另外，为了进一步巩固安全性，还有如下面的公知例那样每隔一定时间就使公用密钥变化的技术。

[0003] 另外，也有 WEP(Wired Equivalent Privacy，有线等效保密）和 WPA(Wi-Fi Protected Access，Wi-Fi 保护访问）等的安全方式。

[0004] 根据这些技术，一般是通过在服务器中发出控制命令来进行认证处理。

[0005] 另外，也公开了一种技术，在通信系统中，保持客户端侧的密码不变而只变更服务器的控制变量，由此来变更共有的加密密钥。由此，能够以较短的时间间隔使共有的公用密钥变化从而提高了密码系统的安全性。

[0006] 专利文献 1 ：日本特开平 9-321748 号公报

[0007] 与有线还是无线无关，在考虑包含非常多的节点装置的网络的情况下，1 个管理服务器生成公用密钥（也就是说根据时间变更）并向各节点装置通知并不实用。即，由于节点装置的数量较多，所以即使只是从服务器发送控制指令也会造成大量负荷。因此，希望各节点装置与其他节点装置协同动作自主地进行用于加密的动作。

发明内容

[0008] 本发明的目的在于，提供一种与其他节点装置协同动作自主地进行用于加密的动作的节点装置，以及命令节点装置与其他节点装置协同动 作自主地进行用于加密的动作的程序。

[0009] 第 1 方式的节点装置是由包含第 1 节点装置和第 2 节点装置的多个节点装置构成的网络中的上述第 1 节点装置，具有访问密钥生成部、公用密钥生成部、访问密钥通知部、访问密钥接收部、访问密钥解密部、数据发送部、数据接收部、数据解密部以及一致性确认部。

[0010] 上述访问密钥生成部每隔第 1 时间变更生成作为上述第 1 节点装置中固有的加密密钥的第 1 访问密钥。另外，上述公用密钥生成部每隔在上述多个节点装置中是共同的时间的第 2 时间变更生成在上述网络内的上述多个节点装置中公用的公用密钥。

[0011] 上述访问密钥通知部使用所生成的上述公用密钥对生成的上述第 1 访问密钥进行加密并向上述第 2 节点装置发送。上述访问密钥接收部接收从上述第 2 节点装置发送来的包含访问密钥通知数据的访问密钥通知帧，该访问密钥通知数据是使用上述公用密钥对作为上述第 2 节点装置所固有的加密密钥的第 2 访问密钥进行加密而得到的数据。

[0012] 上述访问密钥解密部使用所生成的上述公用密钥对上述访问密钥通知数据解密，由此从上述访问密钥通知数据中取得上述第 2 访问密钥。

[0013] 上述数据发送部向第 1 明文帧附加使用上述公用密钥对包含根据该第 1 明文帧计算出的第 1 散列 (hash) 值的数据进行加密得到的第 1 署名数据。并且，上述数据发送部使用解密得到的上述第 2 访问密钥对附加有上述第 1 署名数据的上述第 1 明文帧进行加密并作为第 1 加密帧发送。

[0014] 上述数据接收部从上述第 2 节点装置接收第 2 加密帧。这里，上述第 2 加密帧，是利用上述第 1 访问密钥对第 2 明文帧进行加密得到的，该第 2 明文帧附加有使用上述公用密钥对包含第 2 散列值的数据进行加密得到的第 2 署名数据。

[0015] 上述数据解密部使用上述第 1 访问密钥对上述第 2 加密帧进行解密，从而从上述第 2 加密帧中得到附加有上述第 2 署名数据的上述第 2 明文帧。

[0016] 上述一致性确认部通过使用所生成的上述公用密钥对上述第 2 署名数据解密来取得上述第 2 散列值。并且，上述一致性确认部根据上述第 2 明文帧计算第 3 散列值，并确认是否取得了上述第 2 散列值和上述第 3 散列值之间的一致性。

[0017] 第 2 方式的程序是由控制由包含第 1 节点装置和第 2 节点装置的多个节点装置构成的网络中的上述第 1 节点装置的计算机执行的程序。上述程序是使上述计算机控制第 2 方式的上述第 1 节点装置以使得第 2 方式的上述第 1 节点装置与第 1 方式的上述第 1 节点装置同样地进行动作的程序。

[0018] 在上述任何一个方式中，网络中的第 1 节点装置能够自主地并且与第 2 节点装置等其他节点装置协同动作来进行为了加密通信的动作。所以，上述任何一个方式，都能够提高包含多个节点装置的网络中的通信的安全性。

附图说明

[0019] 图 1 是自组织 (ad hoc) 通信系统的整体概念图。

[0020] 图 2 是表示包含多个节点装置的传感器网络的例子的网络构成图。

[0021] 图 3 是实施方式涉及的节点装置的构成图。

[0022] 图 4 是实施方式涉及的节点装置的硬件构成图。

[0023] 图 5 是更加详细表示本实施方式涉及的节点装置的构成的图。

[0024] 图 6 是对基于实施方式涉及的节点装置的认证方法进行说明的图。

[0025] 图 7 是表示了在 2 个节点装置之间互相认证对方的节点装置并进行通信的处理的顺序图。

[0026] 图 8 是表示数据帧的格式的图。

[0027] 图 9 是公用密钥更新处理的流程图。

[0028] 图 10 是访问密钥更新处理的流程图。

[0029] 图 11 是问候帧发送处理的流程图。

[0030] 图 12 是说明问候帧的格式和进行的与问候帧有关的各种处理的图。

[0031] 图 13 是问候帧接收处理的流程图。

[0032] 图 14 是数据帧发送处理的流程图。

[0033] 图 15 是说明数据帧的格式和进行的与数据帧有关的各种处理的第 1 例的图。

[0034] 图 16 是数据帧接收处理的流程图。

[0035] 图 17 是说明数据帧的格式和进行的与数据帧有关的各种处理的第 2 例的图。

[0036] 图 18 是说明时刻同步方法的图。

[0037] 图 19 是说明时刻同步方法的顺序图。

[0038] 图 20 是时刻同步帧发送处理的流程图。

[0039] 图 21 是时刻同步帧接收处理的流程图。

具体实施方式

[0040] 下面，参照附图对本发明的实施方式进行详细说明。图 1 是自组织通信系统的整体概略图。如图 1 所示那样，节点装置 (a、b、...、s、t) 相互连接构成网。在自组织通信系统中，各节点装置作为中继器工作，将信息从开始节点 (图 1 的例中的节点装置 b) 传递到目标节点 (图 1 的例中的节点装置 t)。

[0041] 各节点装置各自保有固有的识别信息 (ID、Identification)、即节点 ID。也可以将 MAC(Media Access Control) 地址作为节点 ID 利用。

[0042] 各节点装置不把握相互邻接的节点装置和网络整体。在初始状态时，相互的链接不存在，各节点装置不把握自身以外的节点装置。

[0043] 所以，在图 1 所示的自组织通信系统中，为了将信息从作为开始节点的节点装置 b 传递到作为目标节点的节点装置 t，首先需要决定路径。决定路径的顺序如下面所述。

[0044] 首先，各节点装置检测周围的节点装置。为此各节点装置周期性地向邻近存在的节点装置通知自身的存在。在针对邻近节点装置的通知中附带有与路径生成有关的信息。各节点装置若从其他的节点装置接收到了通知，则能够生成关于周围的节点装置的列表，并把握自身节点装置的周围存在的其他节点装置。

[0045] 检测出周围的节点装置的节点装置根据所生成的列表决定自身节点装置要转送信息的节点装置，并向该决定的节点装置转送信息。

[0046] 各节点装置，由于安全对策的原因，将帧加密后与对方的节点装置通信。具体来讲，各节点装置使用通信对方的节点装置所固有的加密密钥和网络中的节点装置之间公用的公用密钥进行加密，并将信息发送至通信对方的节点装置。另外，各节点装置若从通信对方的节点装置接收到了信息，则使用自身节点装置所固有的加密密钥和上述的公用密钥对帧进行解密来取出信息。

[0047] 后面同样，在节点装置间的通信中，各节点装置使用解密得到的加密密钥将数据发送至通信对方的节点装置。另外，各节点装置根据接收到的数据是利用自身节点装置生成的加密密钥被加密了的情况判断通信对方的节点装置是合法的。

[0048] 下面，具体说明基于本实施方式涉及的节点装置的认证处理以及通信的方法。

[0049] 本实施方式的节点装置能够应用于如图 1 那样的任意的自组织通信系统中，也可以应用于例如如图 2 那样的通过自组织网络实现的传感器网络中。

[0050] 图 2 是表示包含多个节点装置的传感器网络的例子的网络构成图。

[0051] 在图 2 的传感器网络中，多个节点装置 1A ～ 1I 以及网关装置 GW 构成了自组织网络。另外，网关装置 GW 例如通过电缆与服务器 SV 连接。当然，网关装置 GW 和服务器 SV 之间的连接也可以是经由网络的连接，也可以是基于无线的连接。

[0052] 在图 2 中，多个节点装置 1A ～ 1I 各自或者与未图示的 1 个以上的传 感器连接，或者内置有未图示的 1 个以上的传感器。后面为了使说明简单，设各节点装置 1A ～ 1I 各

自与 1 个传感器连接。传感器例如也可以是感知温度、压力、加速度等的传感器。另外，也可以使用不同种类的多个传感器。

[0053] 各节点装置 1A ～ 1I 从与自身节点装置连接的传感器取得表示传感器感知的结果的数据（后面称为“传感器数据”）。并且，各节点装置 1A ～ 1I 生成包含所取得的传感器数据的加密帧（后面称为“传感器数据帧”），通过自组织网络向网关装置 GW 发送传感器数据帧。

[0054] 例如，各传感器也可以在 1 分钟内向节点装置输出一次传感器数据。所以，在如上所述那样节点装置 1A ～ 1I 分别与 1 个传感器连接的情况下，各节点装置 1A ～ 1I 在 1 分钟内发送 1 次传感器数据帧。

[0055] 网关装置 GW 和各节点装置 1A ～ 1I 一样具备后面说明的图 3 的各部，能够和节点装置 1A ～ 1I 协同动作自主地构成自组织网络。也就是说，在节点装置 1A ～ 1I 和网关装置 GW 之间，公用密钥是公用的，后面说明的时刻同步用的固定密钥也是公用的。

[0056] 网关装置 GW 将由各节点装置 1A ～ 1I 发送来的传感器数据帧中包含的传感器数据发送至服务器 SV。例如，网关装置 GW 也可以如下面那样动作。

[0057] 网关装置 GW 对接收到的传感器数据帧进行解密并提取传感器数据。并且，网关装置 GW 向服务器 SV 发送包含提取出的传感器数据的数据。

[0058] 或者，网关装置 GW 也可以进一步从接收到的传感器数据帧中提取传感器数据帧的发送源的节点装置（1A ～ 1I 中的任意一个）的识别信息。并且，网关装置 GW 也可以生成将对包含传感器数据和识别信息的数据进行加密而得到的数据包含在净荷中的加密帧并向服务器 SV 发送。

[0059] 服务器 SV 能够使用收集到的传感器数据进行基于传感器感知的物理量的任意的各种处理。例如，在各传感器是温度传感器的情况下，服务器 SV 也可以进行分析温度分布和温度变化的处理，还可以进行温度预测处理。

[0060] 如果将后面详细说明的本实施方式的节点装置 1 作为图 2 的节点装置 1A ～ 1I 利用，则服务器 SV 能够在将传感器数据保持秘密状态的同时对其进行收集，并且能够收集未经篡改的正确的传感器数据。

[0061] 图 3 是本实施方式涉及的节点装置的构成图。图 3 所示的节点装置 1 具有访问密钥生成部 2、公用密钥生成部 3、加密部 4、解密部 5、帧处理部 6、发送部 7、接收部 8 以及时刻同步部 9。例如，图 2 的节点装置 1A ～ 1I 各自具有图 3 那样的构成。

[0062] 访问密钥生成部 2 生成节点装置 1 所固有的加密密钥（后面称为“访问密钥”）。使用公知的 WEP 和 WPA 等技术生成访问密钥。作为对称密钥加密方式中的加密密钥生成访问密钥并使用。

[0063] 另外，每隔规定的时间间隔 t_1 随机更新访问密钥。在本实施方式中，例如 $t_1 = 10$（分钟）。

[0064] 另外，访问密钥通过 RC4(Rivest’s Cipher 4) 被加密并发送至其他的节点装置，在本实施方式中，访问密钥的长度是 128 位。由于 RC4 是流加密的 1 种，所以通过 RC4 加密的密文 (ciphertext) 的长度等于原先的明文 (plaintext) 的长度。

[0065] 但是，一般来说，密钥的长度是 64 位的 RC4 的解读需要收集 50 万帧，密钥的长度是 128 位的解读需要收集 100 万帧。对此，如上所述，在本实施方式中，访问密钥每隔 $t_1 =$

10 分钟随机地变化。

[0066] 例如，如与图 2 相关的示例那样，若设通常每分钟发送 1 帧，则 10 分钟内发送 10 帧。并且，例如，在图 2 的例子中，作为传感器数据帧的最终发送目的地的网关装置 GW 在自组织网络内接收最多的帧。但是，即使是网关装置 GW，例如从总数 500 台的节点装置接收数据的情况下的帧数是每分钟大约 500 帧。即，在访问密钥被更新之前的 10 分钟内，非法节点装置收集解读所需要的帧，可以说事实上是不可能的。

[0067] 公用密钥生成部 3 通过节点装置 1 内具备的防篡改装置（例如后面说明的图 4 的防篡改 PIC 微机 14）等生成在图 1 的网络内的节点装置中公用的加密密钥、即公用密钥。公用密钥每隔规定的时间间隔 t_2 被更新。在本实施方式中，例如 $t_2 = 12$（小时）。

[0068] 在各节点装置中保有的时刻信息在网络内被同步。因此，公用密钥虽然根据时间变化，但是在某个时刻，在网络内的节点装置中是共同的。

[0069] 加密部 4 对向其他节点装置发送的帧中包含的数据进行加密，解密部 5 对由其他节点装置加密并发送的帧中包含的数据进行解密。

[0070] 发送部 7 向其他节点装置发送包含在图 3 所示的节点装置 1 中生成的加密数据的加密帧，接收部 8 接收其他节点装置发送的加密帧。

[0071] 帧处理部 6 执行对接收到的帧的处理。例如，帧处理部 6 也可以从接收到的帧的规定的字段取出信息，进行“是否是已经接收过的帧”的判断作为上述“对接收到的帧的处理”。或者，帧处理部 6 也可以从接收到的帧的规定的字段取出信息，进行“是否是由合法的节点装置发送的帧”的判断等作为上述“对接收到的帧的处理”。

[0072] 帧处理部 6 还进行生成要发送的帧的处理。时刻同步部 9 执行用于使图 3 所示的节点装置 1 中保持的时刻与网络内的其他节点装置的时刻同步的处理。与图 18 ～图 21 一起详细说明时刻同步部 9 的动作。

[0073] 图 3 所示的节点装置 1 在开始与网络内的其他节点装置通信之前，在与对方的节点装置之间交换使用公用密钥加密后的访问密钥。利用公用密钥加密的访问密钥被保存在例如被称为“问候帧 (hello frame)”的规定形式的帧的规定字段中，并被向对方的节点装置发送。

[0074] 另外，下面为了方便说明，有时将节点装置 1 自身生成的访问密钥称为“内部来源 (internally-originated) 访问密钥”，将从其他的节点装置接受的访问密钥称为“外部来源 (externally-originated) 访问密钥”。

[0075] 图 3 的节点装置 1 使用自身节点装置 1 中保有的公用密钥对从通信对方的节点装置（具有与图 3 的节点装置 1 相同的构成的未图示的第 2 节点装置）接收的被加密后的访问密钥进行解密。并且，图 3 的节点装置 1 在之后与该未图示的第 2 节点装置进行通信时，使用通过解密得到的访问密钥（即外部来源访问密钥）对发往未图示的第 2 节点装置的帧进行加密。

[0076] 如上所述，公用密钥以及访问密钥分别以规定的时间间隔 t_2 以及 t_1 被更新。因此，即使第三者非法取得了某个时间点上的公用密钥或者访问密钥，也无法进行冒充等的非法访问。

[0077] 接着，参照图 4 对实现图 3 的构成的硬件的具体例进行说明。图 4 是本实施方式涉及的节点装置 1 的硬件构成图。

[0078] 图 3 的节点装置 1 具备 MPU(MicroProcessing Unit)11、有线 PHY(PHYsical layer) 处理部 12、定时器 IC(Integrated Circuit)13、防篡改 PIC(Peripheral Interface Controller) 微机 (microcomputer)14。节点装置 1 还具备 DRAM(Dynamic Random Access Memory)15、闪存 16 和无线 LAN(Local Area Network) 处理部 17。

[0079] MPU11 和有线 PHY 处理部 12 之间的连接接口例如是 MII(Media Independent Interface)/MDIO(Management Data Input/Output)18(另外,“MII/MDIO”是指“MII 或者 MDIO”)。MII 和 MDIO 都是物理层和 MAC 子层 (Media Access Control sublayer) 之间的接口。

[0080] 另外,定时器 IC13 和防篡改 PIC 微机 14 通过 I^2C(Inter-Integrated Circuit)/PIO(Parallel Input/Output) 总线 19 与 MPU11 连接 (另外“I^2C/PIO 总线”是指“I^2C 总线或者 PIO 总线”)。

[0081] DRAM15、闪存 16 和无线 LAN 处理部 17 通过 PCI(Peripheral Component Interconnect) 总线 20 与 MPU11 连接。

[0082] MPU11 通过将作为非易失性存储装置的 1 种的闪存 16 上保存的固件等的各种程序加载到 DRAM15 上并执行来执行各种各样的处理。MPU11 例如执行防篡改 PIC 微机 14 的驱动和用于使节点装置 1 执行后面说明的各种处理的固件程序等的各种各样的程序。

[0083] 另外,DRAM15 中也可以保存加密密钥等各种数据。另外,DRAM15 也可以作为帧的发送缓冲以及接收缓冲使用。闪存 16 如上所述保存固件程序等。另外,闪存 16 中也可以保存节点装置 1 自身所固有的信息 (例如,节点 ID 和 MAC 地址)。

[0084] 有线 PHY 处理部 12 是进行有线连接时的物理层的处理的电路。另外,无线 LAN 处理部 17 是进行无线 LAN 连接时的物理层的处理的硬 件。无线 LAN 处理部 17 例如包含天线、ADC(Analog-to-Digital Converter)、DAC(Digital-to-Analog Converter)、调制器和解调器等,进行物理层和 MAC 子层的处理。所以,在本实施方式中,节点装置 1 能够进行有线通信和无线通信两者。但是,节点装置 1 也能够是只进行有线通信或者无线通信的其中一者的实施方式。

[0085] 定时器 IC13 是直到经过所设定的时间为止进行计时动作,若经过了所设定的时间则输出中断信号的电路。

[0086] 防篡改 PIC 微机 14 是内部具有生成公用密钥的规定的算法的微机。由于防篡改 PIC 微机 14 是防篡改的,所以从外部无法分析生成公用密钥的规定的算法具体是什么样的算法。

[0087] 接着,参照图 5 对参照图 3 和图 4 说明过的节点装置 1 的构成进行更加详细的说明。图 5 是更加详细表示本实施方式涉及的节点装置 1 的构成的图。

[0088] 在图 5 中,表示了和图 3 同样的访问密钥生成部 2、公用密钥生成部 3、加密部 4、解密部 5、帧处理部 6、发送部 7、接收部 8 以及时刻同步部 9。

[0089] 如图 5 所示那样,接收部 8 具备对节点装置 1 接收到的帧根据帧的种类进行分类的帧分支处理部 21 和对应不同帧种类的接收缓冲。例如通过图 4 的 DRAM15 实现接收缓冲。

[0090] 在本实施方式中,具体来说,对应问候帧、时刻同步帧以及数据帧这 3 种种类,接收部 8 具备问候帧接收缓冲 22、时刻同步帧接收缓冲 23 和数据帧接收缓冲 24。

[0091] 例如通过图4的无线LAN处理部17和MPU11或者通过有线PHY处理部12和MPU11来实现帧分支处理部21。如与图12、图15以及图17一起在后面说明的那样，由于帧头包含表示帧的种类的“帧类型”字段，所以帧分支处理部21能够根据帧类型字段的值来识别接收到的帧的种类从而对接收到的帧进行分类。

[0092] 另外，解密部5对应3种帧的种类具备问候帧解密部25、时刻同步 帧解密部26和数据帧解密部27。在本实施方式中通过MPU11实现解密部5，但是也可以通过专用的硬件电路来实现。

[0093] 问候帧解密部25对问候帧接收缓冲22中保存的问候帧进行解密，提取图4中未图示的其他的节点装置的访问密钥并输出。时刻同步帧解密部26对时刻同步帧接收缓冲23中保存的时刻同步帧进行解密，将解密得到的信息发送至时刻同步部9。数据帧解密部27对数据帧接收缓冲24中保存的数据帧进行解密。

[0094] 并且，节点装置1具备图5所示的、保存其他节点装置用的访问密钥（即外部来源访问密钥）的访问密钥保存部28。访问密钥保存部28中保存有由问候帧解密部25解密后的明文中包含的外部来源访问密钥。更具体来讲，访问密钥保存部28将分别与多个节点装置对应的外部来源访问密钥与识别多个节点装置的信息（例如节点ID或者MAC地址等）建立对应关系并保存。

[0095] 另外，例如通过图4的DRAM15来实现访问密钥保存部28。另外，也可以将至少一部分通过MPU11内的高速缓存来实现。

[0096] 另外，节点装置1包含确认解密后的数据帧的正确性的确认部29。确认部29的详细动作和图16一起在后面说明，例如通过MPU11来实现确认部29。另外，在本实施方式中，确认部29也进行解密后的访问密钥的正确性的确认。

[0097] 另外，帧处理部6包含接收数据帧处理部30，进行使用了由确认部29确认为″正确（即没有被篡改）″的数据帧的处理。例如，接收数据帧处理部30可以进行判别是再次接收了和已经接收的数据帧相同的数据帧还是接收了新的数据帧的处理。也可以通过MPU11来实现接收数据帧处理部30。

[0098] 另外，在上述的数据帧解密部27的解密中，使用了节点装置1自身的访问密钥。因此，节点装置1还具备保存自身节点装置1用的访问密钥（即内部来源访问密钥）的访问密钥保存部31。例如也可以通过DRAM15来实现访问密钥保存部31，还可以通过MPU11内的高速缓存来实现。

[0099] 另一方面，在上述的问候帧解密部25的解密中，使用了网络内的多个节点装置中公用的公用密钥。因此，节点装置1还具备保存公用密钥的公用密钥保存部32。例如也可以通过DRAM15来实现公用密钥保存部32，还可以通过MPU11内的高速缓存来实现。

[0100] 另外，如关于图3所说明的那样通过公用密钥生成部3生成公用密钥保存部32中保存的公用密钥。即，根据本实施方式，在多个节点装置的各自的公用密钥生成部3中，按照相同的算法生成根据时刻唯一决定的公用密钥，以使得在多个节点装置之间不需交换公用密钥。

[0101] 另外，为了防止公用密钥的泄露，通过图4的防篡改PIC微机14来实现本实施方式的公用密钥生成部3。即，公用密钥生成部3是防篡改的。

[0102] 另外，公用密钥生成部3为了生成公用密钥利用时刻信息。具体来讲，节点装置1

具备时钟 33，公用密钥生成部 3 参照时钟 33 得到时刻信息。

[0103] 另外，在后面会和图 10 一起详细说明，节点装置 1 还具备通过图 4 的定时器 IC13 实现的计数器 34。计数器 34 反复进行递增计数动作，若计数器 34 的值达到了预先设定的值，则访问密钥生成部 2 生成访问密钥，计数器 34 被清零。

[0104] 另外，在上述的时刻同步帧解密部 26 的解密中，使用在网络内的多个节点装置中公用的、也不随时间变动的、固定的时刻同步密钥。因此，节点装置 1 还具备保存时刻同步密钥的时刻同步密钥保存部 35。

[0105] 时刻同步密钥，例如可以作为常数预先写入 MPU11 执行的固件程序中，通过将固件加载到 DRAM15 中来保存储 DRAM15 中。例如能够通过闪存 16、DRAM15 或者 MPU11 内的高速缓存来实现时刻同步密钥保存部 35。

[0106] 但是，帧处理部 6 不止是处理接收到的数据帧的上述的接收数据帧处理部 30，还具备生成问候帧的问候帧生成部 36。问候帧生成部 36 从访问密钥保存部 31 中读取节点装置 1 自身的访问密钥，生成问候帧的原来的明文帧并输出。例如通过 MPU11 来实现问候帧生成部 36。

[0107] 问候帧生成部 36 输出的明文帧被输入到加密部 4 进行加密。另外，加密部 4 具备问候帧加密部 37、时刻同步帧加密部 38 以及数据帧加密部 39，例如也通过 MPU11 来实现加密部 4 内的这些各部。

[0108] 问候帧加密部 37 使用公用密钥保存部 32 中保存的公用密钥对问候帧的原来的明文帧进行加密。另外，时刻同步帧加密部 38 使用时刻同步密钥保存部 35 中保存的时刻同步密钥对时刻同步帧的原来的明文帧进行加密。并且，数据帧加密部 39 使用访问密钥保存部 28 中保存的访问密钥中的作为数据帧的发送目的地的节点装置用的访问密钥对数据帧的原来的明文帧进行加密。

[0109] 另外，如后面与图 20 一起详细说明的那样，从时刻同步部 9 向时刻同步帧加密部 38 输出时刻同步帧的原来的明文帧。

[0110] 另外，帧处理部 6 还具备生成数据帧的原来的明文帧并向数据帧加密部 39 输出的数据帧生成部 40

[0111] 在加密部 4 中被加密的各种帧被输出至发送部 7 并从节点装置 1 发送。具体来讲，发送部 7 除了具备例如通过图 4 的 DRAM15 实现的 3 个缓冲（即问候帧发送缓冲 41、时刻同步帧发送缓冲 42 和数据帧发送缓冲 43），还具备发送处理部 44。例如可以通过有线 PHY 处理部 12 和 MPU11 来实现发送处理部 44，也可以通过无线 LAN 处理部 17 和 MPU11 来实现。

[0112] 问候帧发送缓冲 41 从问候帧加密部 37 接受被加密的问候帧并保存，并向发送处理部 44 输出。时刻同步帧发送缓冲 42 从时刻同步帧加密部 38 接受被加密的时刻同步帧并保存，并向发送处理部 44 输出。数据帧发送缓冲 43 从数据帧加密部 39 接受被加密的数据帧并保存，并向发送处理部 44 输出。并且，发送处理部 44 发送接受到的帧。

[0113] 另外，如图 5 所示那样，节点装置 1 例如还具备通过 DRAM15 实现的最新发送时刻保存部 45，因为在后面会与图 16 一起说明最新发送时刻保存部 45，所以这里省略其说明。

[0114] 上面参照图 3 ～图 5 对节点装置 1 的构成进行了说明，因此接着参照图 6 ～图 21 对节点装置 1 的动作进行说明。

[0115] 图 6 是说明基于本实施方式涉及的节点装置 1 的认证方法的图。

[0116] 如图 6 所示那样，当在节点装置 1A 的周边存在节点装置 1B 以及节点装置 1C 的情况下，节点装置 1A 将生成的访问密钥 a1 分别与节点装置 1B 以及节点装置 1C 的访问密钥 b1 以及 c1 交换。并且，节点装置 1A 利用访问密钥 b1 对数据帧加密并向节点装置 1B 发送，利用访问密钥 c1 对数据帧加密并向节点装置 1C 发送。

[0117] 在图 6 的例子中，对于节点装置 1A，访问密钥 a1 是内部来源访问密钥、访问密钥 b1 以及 c1 是外部来源访问密钥。另一方面，对于节点装置 1B，访问密钥 a1 是外部来源访问密钥，访问密钥 b1 是内部来源访问密钥。

[0118] 节点装置 1A 对于节点装置 1B 和节点装置 1C 使用分别不同的访问密钥 (b1 以及 c1)。另外，例如，在与节点装置 1B 的通信中，节点装置 1A 在数据发送时使用访问密钥 b1 而在数据接收时使用访问密钥 a1。这样，节点装置 1A 在数据发送时和数据接收时分别使用不同的访问密钥进行通信。换言之，内部来源访问密钥是解密用的密钥，外部来源访问密钥是加密用的密钥。

[0119] 这样，构成自组织通信网络的节点装置各自通过上述的方法与邻接的节点装置交换访问密钥，使用从通信对方的节点装置接收的访问密钥对帧加密并发送。另外，与此同时，对从通信对方接收到的帧，使用在自身节点装置中被定期更新的访问密钥进行解密。由此，确保了安全性。

[0120] 如上所述，在本实施方式中，网络内的各节点装置在与邻接的节点装置进行通信时，生成用于使通信对方的节点装置访问自身节点装置的访问密钥。并且，各节点装置使用网络中公用的公用密钥，对上述生成的访问密钥进行加密，并将加密后的访问密钥利用问候帧广播。各节点装置使用公用密钥对从邻接节点装置接收到的问候帧中包含的访问密钥进行解密，使用解密后得到的访问密钥访问邻接节点装置。下面，对 2 台节点装置之间执行的处理进行具体说明。

[0121] 图 7 是表示了在 2 个节点装置之间互相对对方的节点装置进行认证并通信的处理的顺序图。这里，为了互相区别 2 台节点装置 1，分别设 为“节点装置 1A”以及“节点装置 1B”。

[0122] 首先，在步骤 S1 中，从节点装置 1A 向作为通信对方节点装置的节点装置 1B 发送由节点装置 1A 生成的访问密钥 a1。访问密钥 a1 如上面所述的那样被利用节点装置 1A 和节点装置 1B 之间共同保有的公用密钥加密。节点装置 1B 使用在自身节点装置 1B 中使用防篡改装置生成的公用密钥进行解密处理，得到访问密钥 a1。

[0123] 接着，在步骤 S2 中，从节点装置 1B 向作为通信对方节点装置的节点装置 1A 发送由节点装置 1B 生成的访问密钥 b1。访问密钥 b1 也被利用节点装置 1A 和节点装置 1B 之间公用的公用密钥加密。节点装置 1A 使用在自身节点装置 1A 中使用防篡改装置生成的公用密钥进行解密处理，得到访问密钥 b1。

[0124] 在步骤 S1 以及步骤 S2 的处理中，在一方的节点装置是企图非法访问的第三者的情况下，和通信对方节点装置之间没有公用的公用密钥，无法解密并取得通信对方节点装置的访问密钥。利用此，当在 2 台的节点装置 1A 和 1B 之间进行了访问密钥的交换的情况下，能够判断通信对方的节点装置 1A 以及 1B 合法。也就是说，当在节点装置 1A 和 1B 之间进行了访问密钥的交换的情况下，节点装置 1A 能够判断节点装置 1B 合法，节点装置 1B 能够判断节点装置 1A 合法。

[0125] 在本实施方式中，设根据与通信对方节点装置之间的访问密钥的交换的成功与否来进行通信对方节点装置的认证，在认证成功的情况下，开始步骤 S3 之后的通信。

[0126] 另外，在每次访问密钥被更新时执行步骤 S1 以及步骤 S2 的认证处理。

[0127] 在步骤 S3 中，从节点装置 1A 向节点装置 1B 发送包含数据的帧。发送的帧被利用在步骤 S2 中节点装置 1A 取得的访问密钥 b1 加密。例如，如关于图 2 所说明的那样，作为包含传感器数据的加密帧的传感器数据帧在步骤 S3 中被发送。

[0128] 另外，在帧中进行了署名。关于署名会在后面说明。接收到帧的节点装置 1B 使用在自身节点装置 1B 中生成的访问密钥 b1 对接收到的帧 进行解密，得到数据。

[0129] 在步骤 S4 中，从节点装置 1B 向节点装置 1A 发送包含数据的帧。发送的帧被利用在步骤 S1 中节点装置 1B 取得的访问密钥 a1 加密并被署名。在接收到帧的节点装置 1A 中，使用在自身节点装置 1A 中生成的访问密钥 a1 对接收到的帧进行解密，得到数据。

[0130] 如图 7 所示那样，本实施方式涉及的节点装置 1(1A 以及 1B) 使用和通信对方的节点装置 (1B 以及 1A) 公用的公用密钥，对各节点装置 (1A 以及 1B) 中生成的访问密钥 (a1 以及 b1) 进行加密并交换。在通信对方的节点装置 (1B 以及 1A) 合法的情况下，通信对方的节点装置 (1B 以及 1A) 保有和自身节点装置 (1A 以及 1B) 公用的公用密钥。

[0131] 因此，各节点装置 (1A 以及 1B) 能够使用自身节点装置 (1A 以及 1B) 中保有的公用密钥对从通信对方的节点装置 (1B 以及 1A) 接收到的访问密钥 (b1 以及 a1) 进行解密。由于在企图非法访问的第三者中没有保有上述公用密钥，所以各节点装置 (1A 以及 1B) 能够根据是否能够对接收到的访问密钥 (b1 以及 a1) 解密来判断通信对方的节点装置 (1B 以及 1A) 是合法的还是非法的。各节点装置 1 定期与通信对方的节点装置交换访问密钥，继续与被判断为是合法的节点装置进行通信。

[0132] 另外，在接收数据时，使用在自身节点装置中生成的访问密钥进行解密处理，并取出数据。例如，在步骤 S3 中，接收侧的节点装置 1B 使用自身节点装置 1B 生成的访问密钥 b1 进行解密处理。

[0133] 在发送数据时，使用在认证处理中从通信对方节点装置接收的、在通信对方节点装置中生成的访问密钥进行加密，并发送数据。例如，在步骤 S3 中，发送侧的节点装置 1A 使用在步骤 S2 中从通信对方节点装置 1B 接收到的访问密钥 b1 进行加密处理。

[0134] 图 8 是表示数据帧的格式的图。后面会和图 15 以及图 17 一起对格式进行更加详细的说明。另外，问候帧的格式的例子会在后面与图 12 一起说明。

[0135] 如图 8 所示那样，数据帧由帧头、帧的识别信息 (FID)、时刻信息以及帧体构成，在数据帧中追加有署名。

[0136] 在帧头中，保存有帧的发送目的地信息等。在 FID 中，保存有由发送源的节点装置 1 附加的用于识别数据帧的顺序编号等。在时刻信息中保存有表示图 8 所示的帧被构成的时刻的信息。具体来讲，保存有表示将图 8 的数据帧向邻接节点装置转送的时刻的信息。在帧体中，保存有数据主体。

[0137] 在署名中，保存有帧（准确来说是明文帧）自身的散列代码被利用公用密钥加密后的值。利用署名来证明图 8 所示的帧是在保有相同的公用密钥的节点装置中生成的。

[0138] 图 8 所示的数据帧被利用通信对方的节点装置的访问密钥（也就是说是外部来源访问密钥）加密并被发送。

[0139] 本实施方式涉及的节点装置 1 若从通信对方的节点装置接收到加密帧，则使用自身节点装置生成的访问密钥进行解密得到明文帧。节点装置 1 还从明文帧中取出作为署名被附加的加密后的散列值，并且使用公用密钥对取出的散列值（被加密的散列值）进行解密。并且，比较使用公用密钥解密得到的值和根据明文帧计算出的散列值，在相互一致的情况下，节点装置 1 判定为“接收了在保有与自身节点装置相同的公用密钥的节点装置中生成的帧”。

[0140] 另外，本实施方式涉及的节点装置 1 预先存储从对方接收到的数据帧的 FID 和时刻信息的组合，将存储的 FID 以及时刻信息与接收到的数据帧的 FID 以及时刻信息进行比较。例如，在被认证为合法的 2 台节点装置之间进行通信时，有时会发生非法的节点装置捕获以及复制数据帧并发送来的情况。在这种情况下，数据帧中包含的 FID 以及时刻信息与过去从合法的节点装置接收到的 FID 以及时刻信息一致。这样，在接受到的数据帧的 FID 以及时刻信息与节点装置 1 自身存储的 FID 以及时刻信息一致的情况下，节点装置 1 判断为是来自非法的节点装置的访问，从而废弃接收到的数据帧。

[0141] 另外，在从合法的节点装置再次发送了数据帧的情况下，虽然 FID 与存储的 FID 一致，但是时刻信息是不同的。这样，对于“FID 与存储的值一致而时间信刻不同”的数据帧，节点装置 1 判断为与已经接收的数据帧相同，从而也废弃该数据帧。

[0142] 接着，对于上述参照图 6 ～图 8 说明的一系列处理，参照图 9 ～图 16 的流程图进行更详细的说明。

[0143] 图 9 是公用密钥更新处理的流程图。在节点装置 1 的电源接入后开始公用密钥更新处理。

[0144] 在步骤 S101 中，图 4 的控制节点装置 1 整体的 MPU11 参照图 5 的时钟 33 识别当前时刻，判断当前时刻是否是预先决定的更新时刻。另外，这里的“更新时刻”是作为进行公用密钥的更新的时刻而预先决定的时刻。例如，在 t_2 ＝ 12（小时）的情况下，也可以决定为“更新时刻是每天 1 点和 13 点”。

[0145] 如果当前时刻是更新时刻，则处理进入步骤 S102。MPU11 命令防篡改 PIC 微机 14 的驱动器（后面称为“防篡改装置驱动器”）开始用于生成公用密钥的处理。防篡改装置驱动器作为公用密钥生成部 3 的一部分工作。

[0146] 即，MPU11 向防篡改装置驱动器提供作为用于生成公用密钥的种子 (seed) 使用的数据（后面称为“种子数据”）作为参数。防篡改装置驱动器也是通过 MPU11 执行的程序的 1 种。

[0147] 接着，在步骤 S103 中，防篡改装置驱动器向作为防篡改装置的防篡改 PIC 微机 14 输出接受到的种子数据，并命令防篡改 PIC 微机 14 使用该种子数据生成新的公用密钥。

[0148] 并且，在步骤 S104 中，防篡改 PIC 微机 14 使用接受到的种子数据生成新的公用密钥，并向防篡改装置驱动器通知所生成的公用密钥。防篡改装置驱动器将生成的新的公用密钥保存在例如在 DRAM15 上实现的公用密钥保存部 32 中。

[0149] 通过以上那样做，如果当前时刻是更新时刻，则更新公用密钥。另一方面，如果当前时刻不是更新时刻，则处理返回到步骤 S101。另 外，也可以通过定时器中断来实现步骤 S101 的分支。

[0150] 接着，参照图 10 对访问密钥的更新进行说明。如关于图 7 所说明的那样，访问密

钥被定期更新。

[0151] 图 10 是访问密钥更新处理的流程图。

[0152] 在步骤 S201 中，节点装置 1 内部的定时器计数器（即通过图 4 的定时器 IC13 实现的图 5 的计数器 34）进行递增计数操作。

[0153] 并且，在步骤 S202 中，访问密钥生成部 2 参照计数器 34 的值判断规定的时间 t_1 ＝ 10 分钟是否已经经过。如果规定的时间 t_1 ＝ 10 分钟已经经过（即计数器 34 的值已经达到作为与 t_1 ＝ 10 分钟相对应的值而被预先设定的值），则处理进入步骤 S203，如果规定的时间 t_1 ＝ 10 分钟还没有经过，则处理返回至步骤 S201。

[0154] 在步骤 S203 中，访问密钥生成部 2 按照规定的算法生成新的访问密钥从而覆盖更新访问密钥保存部 31 中存储的内部来源访问密钥。

[0155] 另外，在步骤 S204 中，进行定时器计数器（也就是说图 5 的计数器 34）的清零动作，之后处理返回至步骤 S201。

[0156] 另外，也可以利用当计数值达到与规定的时间 t_2 相当的值时就被清零的未图示的第 2 计数器（也就是说图 5 的计数器 34 之外的计数器）来实现图 9 的公用密钥更新处理。或者反之，访问密钥生成部 2 也可以通过参照时钟 33 判断当前时刻是否符合访问密钥的更新时刻来实现图 10 的访问密钥更新处理。

[0157] 但是，在包含多数的节点装置 1 的自组织通信系统中，优选地，作为自组织通信系统整体，流量在时间上分散。伴随着访问密钥的更新的问候帧的发送例如能够通过下面的 (1) ～ (3) 在自组织通信系统内从时间上被分散。

[0158] (1) 在图 2 的各节点装置 1A ～ 1I 被设定为，在电源接入后经过共同的规定时间以后开始图 10 的处理的情况下，对各节点装置 1A ～ 1I 错开时刻接入电源。这样，由于基于各节点装置 1A ～ 1I 的访问密钥的更新时刻也分散，所以随着访问密钥的更新而接着产生的问候帧的发送也从时 间上分散而发生。

[0159] (2) 各节点装置 1A ～ 1I 也可以被设定为，在电源接入后经过按每个节点装置 1A ～ 1I 不同的随机的时间以后开始图 10 的处理。例如，也可以在各节点装置 1A ～ 1I 各自的闪存 16 的规定的区域中预先写入上述随机的时间而设定。

[0160] (3) 在各节点装置 1A ～ 1I 中也可以被设定为，上述的规定的时间 t_1 的长度不同。例如作为 MPU11 执行的固件程序中利用的定数来预先设定规定的时间 t_1。

[0161] 若如上述那样通过图 10 的处理生成了访问密钥，则如关于图 7 的步骤 S1 和 S2 所说明的那样，问候帧被发送。所生成的新的访问密钥通过问候帧被通知给邻接的节点装置。

[0162] 所以，下面参照图 11 ～图 13 对问候帧的发送和接受进行详细说明。

[0163] 图 11 是问候帧发送处理的流程图。另外，图 12 是说明问候帧的格式和进行的与问候帧有关的各种处理的图。

[0164] 图 11 的处理是以访问密钥生成部 2 生成了访问密钥为契机开始的。例如，在图 7 的步骤 S1 中节点装置 1A 执行图 11 的处理，在步骤 S2 中节点装置 1B 执行图 11 的处理。例如，访问密钥生成部 2 向问候帧生成部 36 通知访问密钥的生成，由此问候帧生成部 36 开始图 11 的处理。

[0165] 在步骤 S301 中，问候帧生成部 36 生成问候数据（即问候帧的净荷的原来的明文数据）和问候帧的帧头。具体来讲，问候数据包含访问密钥生成部 2 新生成的访问密钥的

数据。

[0166] 例如，问候帧是为了交换访问密钥而预先决定的规定的格式的帧即可，净荷中也可以包含访问密钥以外的各种各样的字段。但是，下面为了使说明简单，对于本实施方式的问候帧，以只在净荷中包含被加密的访问密钥的情况作为例子进行说明。

[0167] 在这种情况下，在步骤 S301 中问候帧生成部 36 能够只是从访问密钥保存部 31 中作为问候数据读取内部来源访问密钥来准备问候数据。 即，在步骤 S301 中准备图 12 的明文访问密钥 D1 作为问候数据。

[0168] 接着，在步骤 S302 中，问候帧生成部 36 计算问候数据的散列值，并将计算出的散列值作为署名附加在问候帧的原来的明文帧的末尾。具体来讲，问候帧生成部 36 根据图 12 的明文访问密钥 D1 计算明文散列值 D2，并将连接了帧头、明文访问密钥 D1 和明文散列值 D2 而得到的明文帧输出至问候帧加密部 37。另外，“明文散列值”的名称是为了表明其与加密后的散列值相比是加密前的原来的散列值的名称。

[0169] 并且，在步骤 S303 中，问候帧加密部 37 参照公用密钥保存部 32 读取公用密钥，并使用公用密钥对在步骤 S302 中附加了署名后的明文帧（准确来讲是明文帧的净荷和帧尾）进行加密。

[0170] 例如，在本实施方式中，作为加密算法采用作为流加密的 1 种的 RC4。所以，在步骤 S303 中，问候帧加密部 37 根据公用密钥生成密钥流，求出由明文访问密钥 D1 和明文散列值 D2 组成的部分与密钥流的异或 (XOR :eXclusive OR)。由此，在步骤 S303 中，生成被加密的净荷以及帧尾。

[0171] 具体来讲，如图 12 所示那样，问候帧加密部 37 根据明文访问密钥 D1 生成加密访问密钥 D3，根据明文散列值 D2 生成加密散列值 D4。另外，在图 12 中，使用了公用密钥的加密或者解密的操作用黑色粗体箭头表示。

[0172] 另外，在步骤 S301 中准备的帧头没有被加密而是保持明文 (cleartext) 的原样被使用。在本实施方式中，例如如图 12 所示那样，在步骤 S301 中准备包含本地收信地址 D5、本地发信地址 D6、帧类型 D7 以及帧大小 D8 的各字段的自组织帧头 D9。

[0173] 所以，在步骤 S303 中，问候帧加密部 37 将自组织帧头 D9 与作为净荷 D10 的加密访问密钥 D3 和作为帧尾 D11 的加密散列值 D4 连接，生成问候帧。并且，问候帧加密部 37 向问候帧发送缓冲 41 输出所生成的问候帧。

[0174] 另外，在本实施方式中，为了向邻接的多个装置（其他的节点装置和网关装置 GW）通知访问密钥，对问候帧进行广播。因此，具体来 讲，本地收信地址 D5 是广播地址，本地发信地址 D6 是节点装置 1 自身的 MAC 地址。

[0175] 另外，帧类型 D7 被设定成表示问候帧的值。帧大小 D8 指定了加密访问密钥 D3 和加密散列值 D4 的长度的和（即明文访问密钥 D1 和明文散列值 D2 的长度的和）。

[0176] 最后，在步骤 S304 中发送部 7 发送问候帧。即，作为步骤 S303 的结果暂时保存在问候帧发送缓冲 41 中的问候帧由发送处理部 44 在步骤 S304 中读取并发送。

[0177] 图 13 是问候帧接收处理的流程图。例如，在图 7 的步骤 S1 中，由于图 2 的节点装置 1A 进行图 11 的处理，所以在与节点装置 1A 邻接的节点装置 1B 中进行图 13 的处理。

[0178] 在节点装置 1B 中，若接收部 8 接收到了问候帧，则帧分支处理部 21 根据自组织帧头 D9 的帧类型 D7 判别“接收到的帧是问候帧”。并且，以该判别为契机开始图 13 的处理。

另外，由帧分支处理部 21 判别为是问候帧的接收帧被暂时保存在问候帧接收缓冲 22 中。

[0179] 在步骤 S401 中，解密部 5 的问候帧解密部 25 参照公用密钥保存部 32 读取公用密钥的数据。并且，问候帧解密部 25 使用公用密钥对保存在问候帧接收缓冲 22 中的问候帧（在本实施方式中准确来说是其净荷和帧尾）进行解密。

[0180] 即，问候帧解密部 25 根据公用密钥生成密钥流，求出由净荷 D10 和帧尾 D11 组成的部分和密钥流之间的 XOR。由此，问候帧解密部 25 根据加密访问密钥 D3 得到解密后的明文访问密钥 D12，并且根据加密散列值 D4 得到解密后的明文散列值 D13。并且，问候帧解密部 25 向确认部 29 输出由自组织帧头 D9、解密后的明文访问密钥 D12 和解密后的明文散列值 D13 组成的明文帧。

[0181] 由此，在步骤 S402 中，确认部 29 从由问候帧解密部 25 输入的明文帧中提取解密后的明文访问密钥 D12。并且，确认部 29 计算解密后的明文访问密钥 D12 的散列值，得到图 12 的计算出的散列值 D14。

[0182] 并且，在步骤 S403 中，确认部 29 比较图 12 的解密后的明文散列值 D13 和计算出的散列值 D14。

[0183] 2 个散列值如果相等，则确认部 29 判断为“OK”，处理转移至步骤 S404。另一方面，2 个散列值如果不同，则确认部 29 判断为“NG”，处理转移至步骤 S405。

[0184] 在步骤 S404 中，确认部 29 用解密后的明文访问密钥 D12 覆盖与本地发信地址 D6 建立有关联的访问密钥保存部 28 内的外部来源访问密钥。其结果，与问候帧的发送源的节点装置相对应的外部来源访问密钥被更新。并且结束图 13 的处理。

[0185] 另一方面，在步骤 S405 中，成为开始图 13 的处理的契机的该问候帧被废弃，结束图 13 的处理。

[0186] 上面参照图 10 ～图 13 对与图 7 的步骤 S1 和 S2 相对应的处理进行了详细说明，因此接着参照图 14 ～图 16 对与图 7 的步骤 S3 和 S4 相对应的处理进行详细说明。

[0187] 图 14 是数据帧发送处理的流程图。在图 7 的步骤 S3 中节点装置 1A 进行图 14 的处理，在步骤 S4 中节点装置 1B 进行图 14 的处理。根据实施方式，例如，也可以以来自与节点装置 1 连接的传感器等的外部机器的输入作为契机开始数据帧发送处理。或者，节点装置 1 也可以按照预先决定的计划进行数据帧发送处理。

[0188] 在本实施方式中，若下面的 (1) ～ (3) 的条件成立，则数据帧生成部 40 开始图 14 的处理。

[0189] (1) 准备作为发送对象的数据（后面称为“对象数据”）。对象数据例如可以由与节点装置 1 连接的外部机器输入，也可以由数据帧生成部 40 生成。作为对象数据的例子，是对图 2 进行说明的传感器数据。

[0190] (2) 决定最终的发送目的地（即自组织网络内的全局发送目的地）。也可以将最终的发送目的地如图 2 的例子那样固定地决定为网关装置 GW，还可以由数据帧生成部 40 动态决定。

[0191] (3) 根据全局发送目的地决定本地发送目的地（即邻接的其他节 点装置中的 1 个）。作为自组织通信系统的构成要素的节点装置 1 能够根据全局发送目的地决定本地发送目的地。

[0192] 另外，如下面那样对上述的 (3) 进行补充。

[0193] 如关于图 1 所说明的那样，作为自组织通信系统的构成要素的节点装置 1 能够生成关于在节点装置 1 自身的周围存在的其他节点装置的列表，并根据列表决定节点装置 1 要转送帧的节点装置。也就是说，在节点装置 1 中安装有根据全局发送目的地决定本地发送目的地并对帧进行路由的功能。

[0194] 例如，图 2 的节点装置 1B 生成关于节点装置 1B 自身的周围存在的其他节点装置 1A、1C 以及 1E 的列表，管理“优选将最终的发送目的地是网关装置 GW 的帧向节点装置 1C 转送”之类的信息。也就是说，节点装置 1B 将全局发送目的地（例如网关装置 GW）与表示和节点装置 1B 自身邻接的装置的本地发送目的地（例如节点装置 1C）建立对应关系并管理，进行帧的路由。例如将全局发送目的地和本地发送目的地建立对应关系的信息存储在图 4 的 DRAM15 中。

[0195] 另外，也可以对将全局发送目的地和本地发送目的地建立对应关系的信息进行加权。通过加权表示对于某个全局发送目的地（例如网关装置 GW）将与节点装置 1B 自身邻接的多个装置（例如节点装置 1A、1C 以及 1E）中的哪个优选作为转送目的地。例如，在图 2 的例子中，与网关装置 GW 与节点装置 1A 的组合的权数相比，网关装置 GW 与节点装置 1C 的组合的权数表示较高的优先级。即，通过加权表示了“对于最终的发送目的地是网关装置 GW 的帧，与向节点装置 1A 或者 1E 转送相比，优选向节点装置 1C 转送”之类的信息。

[0196] MPU11 通过执行固件程序来管理上述的信息并判断是否需要转送接收到的帧。在需要转送的情况下，执行固件程序的 MPU11 参照 DRAM15 根据全局发送目的地决定本地发送目的地，并将所决定的本地发送目的地作为转送目的地来发送帧。

[0197] 这里若返回图 14 的说明，则如上面所述那样，数据帧发送处理在上述 (1) ～ (3) 的条件成立时开始。

[0198] 于是，在步骤 S501 中数据帧生成部 40 计算数据帧的净荷的原来的明文净荷的散列值。数据帧生成部 40 将计算出的散列值附加在明文净荷的末尾作为后面的明文帧尾的一部分。本实施方式在帧尾设有署名。

[0199] 这里，如下面所述，参照图 15 对步骤 S501 进行更加详细的说明。

[0200] 图 15 是说明数据帧的格式和进行的与数据帧有关的各种处理的第 1 例的图。图 15 是对采用一部分与图 8 不同的格式的情况进行的说明。关于采用与图 8 相同的格式的情况，在后面与图 17 一起说明。

[0201] 在步骤 S501 中，数据帧生成部 40 发布新的 FID 作为图 15 的明文 FID/D15。另外，数据帧生成部 40 在步骤 S501 中不仅准备关于上述的条件 (1) 所说明的对象数据，还适当地准备净荷中包含的其他数据。在步骤 S501 中准备的数据也可以是从 DRAM15 或者闪存 16 中读取的数据，还可以是由数据帧生成部 40 生成的数据，也可以是由外部机器输入的数据。

[0202] 例如，数据帧生成部 40 将指定作为数据帧的最终的发送目的地的全局发送目的地的数据和条件 (1) 中准备的对象数据合并来生成明文帧体 D16。

[0203] 另外，在图 14 中没有明示，但是，数据帧生成部 40 在步骤 S501 中还生成自组织帧头 D9。自组织帧头 D9 的形式和问候帧相同。

[0204] 即，在数据帧中，自组织帧头 D9 也包含本地收信地址 D5、本地发信地址 D6、帧类型 D7 以及帧大小 D8。但是，本地收信地址 D5 是如上述的条件 (3) 中所说明的那样决定的 MAC

地址。另外，将帧类型 D7 设定成表示数据帧的值。

[0205] 这样，数据帧生成部 40 在步骤 S501 中生成由自组织帧头 D9、明文 FID/D15 和明文帧体 D16 组成的明文净荷，并根据明文净荷计算图 15 的明文散列值 D17。

[0206] 另外，在步骤 S502 中，数据帧生成部 40 参照时钟 33 取得当前时刻信息，将取得的当前时刻信息作为图 15 的明文时刻 D18 连结在明文散列值 D17 的后面。明文散列值 D17 和明文时刻 D18 组成的部分是加 密署名的原来的明文署名。并且，数据帧生成部 40 向数据帧加密部 39 输出由自组织帧头 D9、明文净荷以及明文署名组成的明文帧。

[0207] 于是，在步骤 S503 中，数据帧加密部 39 参照公用密钥保存部 32 读取公用密钥，并使用公用密钥对明文署名加密来得到加密署名 D21。

[0208] 如上述那样，在本实施方式中采用了 RC4 作为加密算法。所以，在步骤 S503 中，数据帧加密部 39 具体来讲根据公用密钥生成密钥流，求出明文署名和密钥流之间的 XOR。

[0209] 其结果，根据明文散列值 D17 得到加密散列值 D19，根据明文时刻 D18 得到加密时刻 D20。换言之，根据明文署名整体得到由加密散列值 D19 和加密时刻 D20 组成的加密署名 D21。

[0210] 接着，在步骤 S504 中，数据帧加密部 39 使用由上述条件 (3) 决定的发送目的地的节点装置（即、在本地发送目的地地址 D5 中指定了 MAC 地址的节点装置）的访问密钥对明文帧进行加密。即、数据帧加密部 39 参照访问密钥保存部 28 读取发送目的地的节点装置的访问密钥，使用读取的访问密钥对明文净荷和加密署名 D21 进行加密。

[0211] 即，数据帧加密部 39 进行密钥流的生成和 XOR 运算。其结果，数据帧加密部 39 分别地根据明文 FID/D15 生成加密 FID/D22，根据明文帧体 D16 生成加密帧体 D23。另外，数据帧加密部 39 根据加密散列值 D19 生成二重加密散列值 D24，根据加密时刻 D20 生成二重加密时刻 D25。也就是说，根据加密署名 D21 得到相当于帧尾的被二重加密的署名。

[0212] 另外，在图 15 以及图 17 中，用黑色箭头表示基于公用密钥的加密以及解密，用斜线模样的箭头表示基于访问密钥的加密以及解密。

[0213] 如上面那样，生成由加密 FID/D22 和加密帧体 D23 组成的净荷 D26 和由二重加密散列值 D24 和二重加密时刻 D25 组成的作为署名的帧尾 D27。所以，在步骤 S504 中，数据帧加密部 39 将净荷 D26 和帧尾 D27 与自组织帧头 D9 连结生成数据帧，并向数据帧发送缓冲 43 输出。

[0214] 最后，在步骤 S505 中，发送部 7 发送数据帧。即，由发送处理部 44 在步骤 S505 中读取作为步骤 S504 的结果暂时保存在数据帧发送缓冲 43 中的数据帧并发送。

[0215] 图 16 是数据帧接收处理的流程图。在图 7 的步骤 S3 中 1B 进行图 16 的处理，在步骤 S4 中节点装置 1A 进行图 16 的处理。

[0216] 下面，为了方便说明，在图 7 的步骤 S3 中，对节点装置 1B 在接受部 8 中接收利用访问密钥 b1 加密的数据帧的情况进行说明。

[0217] 若上述数据帧被节点装置 1B 接收了，则帧分支处理部 21 根据自组织帧头 D9 的帧类型 D7 判别为“接收到的帧是数据帧”。并且，以该判别为契机开始图 16 的处理。另外，由帧分支处理部 21 判别为是数据帧的接收帧被暂时保存在数据帧接收缓冲 24 中。

[0218] 在步骤 S601 中，解密部 5 的数据帧解密部 27 使用自身节点装置 1B 的访问密钥对接收到的帧进行解密。即，数据帧解密部 27 参照访问密钥保存部 31 读取对节点装置 1B 自

身来说作为内部来源的访问密钥的访问密钥 b1 的数据。并且，数据帧解密部 27 使用访问密钥 b1 对保存在数据帧接收缓冲 24 中的数据帧（在本实施方式中准确来讲是其净荷和帧尾）进行解密。

[0219] 即，数据帧解密部 27 根据访问密钥 b1 生成密钥流，求出密文（也就是由图 15 的净荷 D26 和帧尾 D27 组成的部分）和密钥流之间的 XOR。由此，数据帧解密部 27 根据加密 FID/D22 得到解密后的明文 FID/D28，根据加密帧体 D23 得到解密后的明文帧体 D29。另外，数据帧解密部 27 根据二重加密散列值 D24 得到解密后的密文散列值 D30，根据二重加密时刻 D25 得到解密后的密文时刻 D31。也就是说，数据帧解密部 27 根据二重加密署名得到加密署名。

[0220] 接着，在步骤 S602 中，数据帧解密部 27 参照公用密钥保存部 32 读取公用密钥的数据，使用公用密钥对由解密后的密文散列值 D30 和解密后的密文时刻 D31 组成的加密署名进行解密。其结果，根据解密后的密文散列值 D30 得到解密后的明文散列值 D33，根据解密后的密文时刻 D31 得到解密后的明文时刻 D34。

[0221] 所以，数据帧解密部 27 将自组织帧头 D9、解密后的明文 FID/ D28、解密后的明文帧体 D29、解密后的明文散列值 D33 以及解密后的明文时刻 34 作为解密后的明文帧向确认部 29 输出。

[0222] 在步骤 S603 中，确认部 29 从来自数据帧解密部 27 的输入中提取由解密后的明文 FID/D28 和解密后的明文帧体 D29 组成的部分（后面称为“解密后的明文净荷”）。并且，确认部 29 计算解密后的明文净荷的散列值，得到图 15 的计算出的散列值 D32。

[0223] 在步骤 S603 中，作为接受到的数据帧的认证判定处理，确认部 29 比较计算出的散列值 D32 和解密后的明文散列值 D33。如果接受到的数据帧是没有被篡改过之类的正确的数据帧，则计算出的散列值 D32 和解密后的明文散列值 D33 一致。

[0224] 所以，在计算出的散列值 D32 和解密后的明文散列值 D33 一致的情况下，确认部 29 判定为“OK”，处理转移至步骤 S604。另一方面，在计算出的散列值 D32 和解密后的明文散列值 D33 不一致的情况下，确认部 29 判定为“NG”，处理转移至步骤 S608。

[0225] 在步骤 S604 中，确认部 29 提取解密后的明文时刻 D34。由于步骤 S604 被执行是因为是在步骤 S603 中判断为“OK”的情况，所以解密后的明文时刻 D34 等于原来的明文时刻 D18。另外，确认部 29 在步骤 S604 中也提取本地发信地址 D6。

[0226] 并且，在步骤 S605 中，确认部 29 进行时刻判定处理。时刻判定处理是为了防御冒充攻击的处理。另外，在本说明书中，将非法的第三者监听（即捕获）数据帧，并将监听到的数据帧复制或者变更其中一部分进行发送的情况称为冒充攻击。

[0227] 具体来讲，确认部 29 参照图 5 的最新发送时刻保存部 45 进行时刻判定处理。如图 16 所示那样，最新发送时刻保存部 45 存储将本地发信地址和时刻建立对应关系的项。

[0228] 例如，图 16 所示的第 1 项将本地发信地址 A_1 和时刻 T_1 建立了对应关系。另外，如上所述，图 16 的说明是将节点装置 1B 进行图 16 的处理的情况作为例子。所以，图 16 所示的第 1 项表示“根据节点装置 1B 从利用本地发信地址 A_1 识别的节点装置接收到的最新的数据帧得到 的解密后的明文时刻 D34 是 T_1”。

[0229] 节点装置 1B 的电源被接入的时间点、即初始状态下的最新发送时刻保存部 45 没有存储任何项，但是通过后面说明的步骤 S606 来向最新发送时刻保存部 45 追加项，或者更

新已经存在的项。

[0230] 在步骤 S605 中，确认部 29 将提取出的本地发信地址 D6 作为检索关键字对最新发送时刻保存部 45 进行检索。作为检索的结果，如果不存在“本地发信地址”字段与提取出的本地发信地址 D6 一致的项，则确认部 29 判断为“接收到的数据帧不是通过冒充攻击发送来的数据帧”。即，确认部 29 判断为“接收到的数据帧是合法的数据帧”，处理转移至步骤 S606。

[0231] 相反，作为检索的结果，在找到“本地发信地址”字段与提取出的本地发信地址 D6 一致的项的情况下，接收到的数据帧有可能是通过冒充攻击发送来的。所以，确认部 29 将找到到的项的“时刻”字段的值与在步骤 S604 中提取出的解密后的明文时刻 D34 进行比较。

[0232] 在 2 个时刻一致的情况下，确认部 29 判断为“接收到的数据帧是基于冒充攻击的数据帧”，处理转移至步骤 S608。相反，如果 2 个时刻不一致，则确认部 29 判断为“来自利用本地发信地址 D6 识别的节点装置的、与到目前为止节点装置 1B 接收到的数据帧不同的新的数据帧被合法发送”，处理转移至步骤 S606。

[0233] 在步骤 S606 中，确认部 29 更新利用本地发信地址 D6 识别的发送源节点装置的最新时刻信息。

[0234] 即，在通过步骤 S605 的检索没有找到项的情况下，确认部 29 生成将本地发信地址 D6 和解密后的明文时刻 D34 建立对应关系的新的项并保存在最新发送时刻保存部 45 中。另外，在通过步骤 S605 的检索找到了项的情况下，确认部 29 用解密后的明文时刻 D34 覆盖找到的该项的“时刻”字段的值。

[0235] 若通过上面所述更新了最新发送时刻保存部 45 保持的最新时刻信息，则确认部 29 向接收数据帧处理部 30 输出明文帧。

[0236] 于是，在步骤 S607 中，接收数据帧处理部 30 使用来自确认部 29 的输入进行与实施方式相应的处理。

[0237] 例如，在解密后的明文帧体 D29 中也可以指定对象数据的最终的发送目的地（也就是全局发送目的地）。并且，接收数据帧处理部 30 也可以根据全局的发送目的地判断是否需要转送数据帧，在要转送的情况下决定本地的发送目的地，并命令数据帧生成部 40 构造新的数据帧。

[0238] 另外，接收数据帧处理部 30 也可以如关于图 8 所说明的那样，使用解密后的明文 FID/D28 和解密后的明文时刻 D34 进行非法的数据帧和合法的数据帧的判别和接收到的数据帧是否是再次发送的数据帧的判断。

[0239] 另外，在步骤 S608 中，接收到的数据帧被废弃，结束图 16 的处理。即，在步骤 S608 中，确认部 29 不向接收数据帧处理部 30 输出数据。

[0240] 与上面参照图 14 ～图 16 说明的数据帧的发送接收有关的一系列的处理能够根据数据帧的格式适当地变形。和图 17 一起对其具体例进行说明。

[0241] 图 17 是说明数据帧的格式和进行的与数据帧有关的各种处理的第 2 例的图。图 17 是将图 8 详细化的格式的一例。

[0242] 下面，以从节点装置 1A 向节点装置 1B 发送数据帧的情况为例，对与图 17 对应的处理进行详细说明。

[0243] 节点装置 1A 的数据帧生成部 40 计算由明文 FID/D15、明文时刻 D18 和明文帧体 D16 组成的明文净荷的散列值，得到明文散列值 D35。并且，节点装置 1A 的数据帧加密部 39 使用公用密钥对明文散列值 D35 进行加密得到加密散列值 D36，并使用节点装置 1B 的访问密钥 b1 对由明文净荷和加密散列值 D36 组成的部分进行加密。

[0244] 其结果，根据明文 FID/D15 得到加密 FID/D37，根据明文时刻 D18 得到加密时刻 D38，根据明文帧体 D16 得到加密帧体 D39，根据加密散列值 D36 得到二重加密散列值 D40。

[0245] 节点装置 1A 的数据帧加密部 39 将由加密 FID/D37、加密时刻 D38 和加密帧体 D39 组成的净荷 D41 和作为帧尾 D42 的二重加密散列值 D40 与自组织帧头 D9 连结。通过连结完成的加密数据帧被暂时保存在数据帧发送缓冲 43 中并从发送处理部 44 发送。

[0246] 并且，在接收到了加密后的数据帧的节点装置 1B 中，帧分支处理部 21 根据帧类型 D7 判别为“接收到的帧是数据帧”，并将接受到的帧保存在数据帧接收缓冲 24 中。并且，数据帧解密部 27 利用节点装置 1B 自身的访问密钥 b1 对净荷 D41 和帧尾 D42 进行解密。

[0247] 其结果，根据加密 FID/D37 得到解密后的明文 FID/D43，根据加密时刻 D38 得到解密后的明文时刻 D44，根据加密帧体 D39 得到解密后的明文帧体 D45。另外，根据二重加密散列值 D40 得到解密后的密文散列值 D46。数据帧解密部 27 还通过利用公用密钥对解密后的密文散列值 D46 解密来得到解密后的明文散列值 D48。

[0248] 于是，节点装置 1B 的确认部 29 计算由解密后的明文 FID/D43、解密后的明文时刻 D44 和解密后的明文帧体 D45 组成的部分的散列值，得到计算出的散列值 D47。并且，确认部 29 比较计算出的散列值 D47 和解密后的明文散列值 D48，如果两者不一致则废弃数据帧。

[0249] 计算出的散列值 D47 和解密后的明文散列值 D48 一致时，确认部 29 还将本地发信地址 D6 作为检索关键字对最新发送时刻保存部 45 进行检索，进行与图 16 的步骤 S605 同样的时刻判定处理。步骤 S605 以后的处理和关于图 16 所说明的一样。

[0250] 如上面所述那样，本实施方式涉及的节点装置使用以规定的期间更新的公用密钥交换访问密钥，利用公用密钥以及访问密钥判别是基于第三者的非法的访问还是来自合法的节点装置的访问。因此，需要在节点装置之间使更新公用密钥和访问密钥的定时一致。即，对于节点装置内的时刻，需要在网络内的节点装置之间预先取得同步。下面对时刻的同步方法进行说明。

[0251] 图 18 是说明时刻的同步方法的图。以在图 18 的节点装置 1A 中取得时刻的同步来校准时刻的情况为例进行说明。

[0252] 节点装置 1A 预先将自身节点装置 1A 的当前时刻和进行了时刻校准的最终时刻存储在存储部中（例如 DRAM15）。并且，在接收到了时刻同步用的时刻同步帧的情况下，从时刻同步帧中取出与时刻有关的信息并与在自身节点装置 1A 中存储的信息进行比较。作为比较的结果，在判断为需要进行同步的情况下，节点装置 1A 按照时刻同步帧中包含的信息进行时刻校准。

[0253] 时刻同步帧在本实施方式中是与问候帧类似的格式的控制用帧的 1 种，包含表示当前时刻以及进行了时刻校准的时刻（后面称为“同步时刻”）的数据。这里，当前时刻是指在生成时刻同步帧的时间点上的该节点装置 1 自身的时刻，同步时刻是指在规定的装置中取得了时刻的同步的时刻。所谓规定的装置在本实施方式中是指网关装置 GW，时刻的同步是指在网关装置 GW 中例如通过 SNTP(Simple Network Time Protocol，简单网络时间协

议）等取得时刻的同步。

[0254] 在网关装置 GW 中，定期地、例如每 2 小时一次通过 SNTP 等取得时刻的同步。各节点装置 1 在时刻同步帧中保存自身节点装置 1 的当前时刻和同步时刻并通过时刻同步帧广播。在规定的定时（例如每 2 小时 1 次）使用与上述的时间变化的公用密钥不同的固定的时刻同步密钥对时刻同步帧进行加密并发送。

[0255] 在图 18 所示的例子中，在网关装置 GW 中，在 12 点通过 SNTP 等取得时刻的同步，在 13 点生成时刻同步帧 P1 并发送。

[0256] 接收到时刻同步帧 P1 的节点装置 1A 比较自身节点装置 1A 中存储的最终同步时刻和时刻同步帧 P1 的同步时刻。在图 18 的例子中，时刻同步帧 P1 的同步时刻 (12:00) 比所存储的最终同步时刻 (11:00) 新。在这种情况下，节点装置 1A 作为当前时刻设定接收到的时刻同步帧中保存的当前时刻 (13:00)。

[0257] 这里，节点装置 1A 有时会接收如节点装置 1B 发送的时刻同步帧 P2 那样的、基于不是最新时刻的同步的时刻同步帧。在接收了时刻同步帧 P2 的情况下，由于自身节点装置 1A 中存储的最终同步时刻 (11:00) 比时刻同步帧 P2 的同步时刻 (10:00) 新，所以节点装置 1A 不取得时刻的同步。

[0258] 接着，参照图 19 ～图 21 对图 18 的例子进行更加详细的说明。

[0259] 图 19 是说明参照图 18 说明的时刻的同步方法的顺序图。在图 19 中表示了 SNTP 服务器 SS、网关装置 GW 以及节点装置 1A ～ 1C。下面设为，在自组织网络内网关装置 GW 与节点装置 1A 邻接，节点装置 1A 也与节点装置 1B 以及 1C 邻接。

[0260] 另外，网关装置 GW 和节点装置 1A ～ 1C 都具备图 5 的各部。另外，网关装置 GW 也安装有基于 SNTP 的时刻校准功能。

[0261] 如步骤 S701 所示那样，若网关装置 GW 自身的时钟 33 的时刻变成 12:00，则网关装置 GW 按照预先决定的计划，通过 SNTP 访问 SNTP 服务器 SS，进行时刻校准。

[0262] 另外，在网关装置 GW 中，关于发送时刻同步帧的定时，也预先设定如“13:00 发送”那样的计划。所以，若在步骤 S701 中的时刻校准的结果适当修正的网关装置 GW 的时钟表示成 13:00，则网关装置 GW 如步骤 S702 所示那样发送时刻同步帧 P1。

[0263] 另外，对于发送时刻同步帧的定时，也可以对邻接的多个节点装置分别设定不同的时刻。

[0264] 虽然省略了时刻同步帧的格式的详细的图示，但是时刻同步帧包含和图 12 的问候帧同样的自组织帧头 D9，并且，包含使用时刻同步密钥对包含“同步时刻”和“当前时刻”这两个字段的明文净荷进行加密得到的加密净荷。

[0265] 例如，在步骤 S702 中，网关装置 GW 发送表示“同步时刻是 12:00 而当前时刻是 13:00”的时刻同步帧 P1。即，同步时刻字段的值是网关装置 GW 自身进行了步骤 S701 中的时刻校准的时刻，当前时刻字段的值是网关装置 GW 发送时刻同步帧 P1 的时刻。

[0266] 另外，下面设时刻同步帧 P1 的本地收信地址是节点装置 1A 的地址。后面与图 20 一起详细说明时刻同步帧发送处理。

[0267] 但是，在本实施方式中，在自组织网络内互相邻接的装置之间的通信延迟时间被视为零。于是，当网关装置 GW 的时钟 33 是 13:00 的时 候在节点装置 1A 中接收到时刻同步帧 P1。但是，接收到时刻同步帧 P1 时的节点装置 1A 的时钟 33 例如可能表示为 12:58，

也可能表示为 13:03。

[0268] 所以，接收到时刻同步帧 P1 的节点装置 1A 在步骤 S703 中进行节点装置 1A 自身的时钟 33 的时刻校准（即时刻同步处理）。其结果，节点装置 1A 的时钟 33 被校正到 13:00。另外，步骤 S703 的时刻同步处理具体来讲是图 21 的时刻同步帧接收处理。

[0269] 对于在步骤 S703 中节点装置 1A 的时钟 33 被校正的情况，换言之，也可以说成在步骤 S703 中节点装置 1A 从时间段 Tna1 切换到时间段 Tna2。

[0270] 另外，各个节点装置 1A ～ 1C 根据各个计划设定进行时刻同步帧发送处理。例如，在图 19 的例子中，若节点装置 1B 的时钟变成 13:30，则节点装置 1B 如步骤 S704 所示那样发送时刻同步帧 P2。时刻同步帧 P2 表示“同步时刻是 10:00 而当前时刻是 13:30”。另外，设时刻同步帧 P2 的本地收信地址为节点装置 1A 的地址。

[0271] 由此，节点装置 1A 接收时刻同步帧 P2，并以时刻同步帧 P2 的接收为契机，如步骤 S705 所示那样进行时刻同步处理。但是，与已经在步骤 S703 中进行过的时刻同步处理中使用过的时刻同步帧 P1 中作为同步时刻表示的 12:00 相比，时刻同步帧 P2 中作为同步时刻表示的 10:00 是旧的。因此，如与图 21 一起详细说明的那样，在步骤 S705 中，节点装置 1A 不更新时钟 33。

[0272] 但是，在各个节点装置 1A ～ 1C 中，预先设定了从通过时刻同步处理校正时钟 33 开始到向邻接的其他节点装置发送时刻同步帧为止的间隔 Tnax。例如，对节点装置 1A 设定的间隔 Tnax 是 40 分钟。

[0273] 也可以对每个节点装置 1A ～ 1C 设定不同的随机的间隔。另外，对于节点装置 1A，也可以将从校正时钟 33 开始到向多个节点装置 1B 和 1C 分别发送时刻同步帧为止的间隔设定成相同的值（例如上述的间隔 Tnax）。或者相反，也可以在 1 个节点装置 1A 中将从校正时钟 33 开始到向节点装置 1B 发送时刻同步帧为止的间隔（在图 19 中没有图示）和 从校正时钟 33 开始到向节点装置 1C 发送时刻同步帧为止的间隔 Tnax 设定成不同的值。

[0274] 节点装置 1A 按照设定，若在校正时钟 33 起经过了规定的时间（即 Tnax ＝ 40 分钟），则如步骤 S706 所示那样进行时刻同步帧发送处理。在步骤 S706 中，发送表示“同步时刻是 12:00 而当前时刻是 13:40”的时刻同步帧 P3。

[0275] 时刻同步帧 P3 表示“同步时刻是 12:00”是因为成为节点装置 1A 校正时钟 33 的契机的时刻同步帧 P1 作为同期时刻表示的是 12:00。另外，时刻同步帧 P3 表示“当前时刻是 13:40”是因为时刻同步帧 P3 是在 13:40 被发送的。

[0276] 并且，若在节点装置 1C 中接收到时刻同步帧 P3，则如步骤 S707 所示那样，节点装置 1C 进行时刻同步处理。

[0277] 图 20 是时刻同步帧发送处理的流程图。例如，分别地在图 19 的步骤 S702 中网关装置 GW 进行图 20 的处理，在步骤 S704 中节点装置 1B 进行图 20 的处理，在步骤 S706 中节点装置 1A 进行图 20 的处理。

[0278] 例如，节点装置 1A 的时刻同步部 9 也可以具备与图 5 的计数器 34 不同的未图示的第 2 计数器。例如能够通过与图 4 的定时器 IC13 类似的硬件电路来实现第 2 计数器。

[0279] 在第 2 计数器中设定有表示间隔 Tnax 的值。并且，时刻同步部 9 当在后面与图 21 一起说明的时刻同步帧接收处理结束时对第 2 计数器清零。当第 2 计数器的计数达到表示间隔 Tnax 的值时，时刻同步部 9 开始图 20 的处理。

[0280] 或者，时刻同步部 9 也可以存储校正时钟 33 的时刻，通过参照时钟 33 来判断从进行了存储的时刻算起是否经过了间隔 Tnax，如果经过了间隔 Tnax 则开始图 20 的处理。

[0281] 若开始了图 20 的处理，则在步骤 S801 中时刻同步部 9 将自身节点装置 1 中保持的最终同步时刻作为同步时刻设定在帧中。

[0282] 时刻同步部 9 将根据最后进行了图 21 的处理时的时刻同步帧的同步 时刻字段得到的时刻作为节点装置 1 自身的“最终同步时刻”例如保持在 DRAM15 上。所以，在步骤 S801 中，时刻同步部 9 在新生成的明文帧的同步时刻字段中设定所保持的最终同步时刻的值。

[0283] 例如在图 19 的例子中，在节点装置 1A 的时刻同步部 9 执行步骤 S706 的情况下，时刻同步部 9 作为最终同步时刻保持成为在步骤 S703 中校正时钟 33 的契机的时刻同步帧 P1 表示的同步时刻、即 12:00。所以，在步骤 S706 调用的图 20 的处理的步骤 S801 中，时刻同步部 9 在新生成的明文帧的同步时刻字段中设定为 12:00。

[0284] 接着，在步骤 S802 中，时刻同步部 9 将自身节点装置 1 的时刻同步帧发送时刻作为“当前时刻”设定在帧中（也就是新生成的明文帧）。更严密来说，将步骤 S802 执行时时钟 33 表示的时刻近似地看做来自节点装置 1 的时刻同步帧发送时刻，并通过时刻同步部 9 将其设定在明文帧的当前时刻字段中。

[0285] 例如，在图 19 的例子中，在节点装置 1A 的时刻同步部 9 执行步骤 S706 的情况下，在步骤 S706 调用的图 20 的处理的步骤 S802 中，时刻同步部 9 在明文帧的当前时刻字段中设定为 13:40。

[0286] 并且，在步骤 S803 中，时刻同步部 9 生成时刻同步帧的帧头，并将所生成的帧头附加在明文净荷（包含同步时刻和当前时刻）的前面。在步骤 S803 中生成的帧头例如是与问候帧的自组织帧头 D9 同样的形式。并且，时刻同步部 9 向时刻同步帧加密部 38 输出由帧头和明文净荷组成的明文帧。

[0287] 于是，在步骤 S804 中，时刻同步帧加密部 38 参照时刻同步密钥保存部 35 读取时刻同步密钥，并使用时刻同步密钥对明文净荷加密。例如，在用于对时刻同步帧进行加密的加密算法也是 RC4 的情况下，在步骤 S804 中，时刻同步帧加密部 38 具体来讲进行密钥流的生成和 XOR 操作。时刻同步帧加密部 38 向时刻同步帧发送缓冲 42 输出由在步骤 S803 中附加的帧头和在步骤 S804 中被加密的净荷组成的时刻同步帧。

[0288] 最后在步骤 S805 中，发送部 7 发送时刻同步帧。也就是说，发送 处理部 44 发送暂时保存在时刻同步帧发送缓冲 42 中的时刻同步帧并结束图 20 的处理。

[0289] 图 21 是时刻同步帧接收处理的流程图。例如，在图 19 的步骤 S703 和 S705 中，节点装置 1A 进行图 21 的处理。以节点装置 1 在接受部 8 中接收帧，接收部 8 的帧分支处理部 21 根据自组织帧头 D9 的帧类型 D7 判别为“接收到的帧是时刻同步帧”为契机开始图 21 的处理。另外，若帧分支处理部 21 判别为“接收到的帧是时刻同步帧”，则接收到的帧被输出至时刻同步帧接收缓冲 23 中并被保存。

[0290] 在步骤 S901 中，时刻同步帧解密部 26 从时刻同步帧接收缓冲 23 中读取时刻同步帧并进行解密。即，时刻同步帧解密部 26 参照时刻同步密钥保存部 35 读取时刻同步密钥，并使用时刻同步密钥对时刻同步帧的被加密的净荷进行解密。

[0291] 在如上面所述那样用于对时刻同步帧进行加密的加密算法也是 RC4 的情况下，时刻同步帧解密部 26 在步骤 S901 中具体来讲进行密钥流的生成和 XOR 操作。

[0292] 另外，解密后，时刻同步帧解密部 26 向时刻同步部 9 输出帧头和通过解密得到的明文净荷。

[0293] 于是，在步骤 S902 中，时刻同步部 9 从明文净荷中提取同步时刻字段的值，并且读取例如在 DRAM15 中保持的最终同步时刻。并且时刻同步部 9 比较提取的同步时刻和读取的最终同步时刻。

[0294] 在同步时刻比最终同步时刻新时，处理转移至步骤 S903。相反，在同步时刻与最终同步时刻相同又或者同步时刻比最终同步时刻旧时，处理转移至步骤 S904。

[0295] 在步骤 S903 中，时刻同步部 9 将时刻同步帧的当前时刻作为自身节点装置 1 的时刻来设定。即，时刻同步部 9 提取时刻同步帧的当前时刻字段的值，并在时钟 33 中设定提取出的值，由此来校正时钟 33 的时刻。并且，结束图 21 的处理。

[0296] 例如，在图 19 的步骤 S703 调用图 21 的处理的情况下，步骤 S903 被执行，时刻同步部 9 校正时钟 33。

[0297] 另外，在步骤 S904 中，时刻同步部 9 废弃时刻同步帧并结束图 21 的处理。例如，在图 19 的步骤 S705 调用图 21 的处理的情况下，步骤 S904 被执行。

[0298] 另外，如关于图 20 以及图 21 所说明的那样，虽然本实施方式的时刻同步帧中没有特别包含署名等的帧尾，但是也可以是利用将明文净荷的散列值作为帧尾进行附加的格式的时刻同期帧的实施方式。

[0299] 在这种情况下，在时刻同步帧发送处理中，时刻同步部 9 进行散列值的计算，时刻同步帧加密部 38 对净荷和帧尾的双方进行加密。另外，在时刻同步帧接收处理中，时刻同步帧解密部 26 对净荷和帧尾的双方进行解密。并且，确认部 29 根据通过解密得到的明文净荷计算散列值，并比较计算出的散列值和通过解密得到的明文散列值，只有在 2 个散列值一致的情况下时刻同步部 9 才执行步骤 S902 以后的处理。

[0300] 在构成自组织通信网络的节点装置数量较多的情况下，在各节点装置取得与网关装置等的规定的 1 个装置的时刻同步的构成中，流量增大。另一方面，根据本实施方式，即使在节点装置数量较多的情况下，各节点装置也如上述的时刻同步方法那样从邻接的节点装置中的已经取得了同步的节点装置接收时刻同步帧来进行时刻校准。因此，根据本实施方式，不增大网络整体的流量各节点装置就能够取得时刻的同步。

[0301] 上面参照图 1 ～图 21 对本实施方式进行了详细的说明，关于本实施方式的节点装置 1 的概况如下面所述。

[0302] 图 3 ～图 5 所示的节点装置 1 是例如如图 2、图 6、图 7、图 18 以及图 19 所示那样由多个节点装置构成的网络中的节点装置中的一个。这里为了方便说明，以多个节点装置中的第 1 节点装置 1A 和第 2 节点装置 1B 为着重点来说明第 1 节点装置 1A 的构成概况。

[0303] 第 1 节点装置 1A 如图 3 以及图 5 所示那样具有每隔第 1 时间就变更并生成作为第 1 节点装置 1A 所固有的加密密钥的第 1 访问密钥的访问密钥生成部 2。这里，所谓“第 1 访问密钥”，例如是图 6 的访问密钥 a1，所谓“第 1 时间”，在上述的实施方式的例子中是 t_1 ＝ 10（分钟）。

[0304] 另外，第 1 节点装置 1A 如图 3 以及图 5 所示那样具有每隔作为在多个节点装置中共同的时间的第 2 时间就变更并生成网络内的多个节点装置中公用的公用密钥的公用密钥生成部 3。这里，所谓“第 2 时间”在上述的实施方式的例子中是 t_2 ＝ 12（小时）。

[0305] 另外，第 1 节点装置 1A 具有作为利用所生成的公用密钥对所生成的第 1 访问密钥进行加密并向第 2 节点装置 1B 发送的访问密钥通知部而工作的组件。即，图 3 的帧处理部 6、加密部 4 和发送部 7 协同动作作为上述访问密钥通知部而工作。更详细来说，图 5 的问候帧生成部 36、问候帧加密部 37、问候帧发送缓冲 41 和发送处理部 44 协同动作作为上述访问密钥通知部而工作。

[0306] 另外，第 1 节点装置 1A 具有作为接收从第 2 节点装置 1B 发送来的访问密钥通知帧的访问密钥接收部而工作的组件。这里，“访问密钥通知帧”包含使用公用密钥对第 2 节点装置 1B 所固有的加密密钥、即第 2 访问密钥进行加密得到的数据、即访问密钥通知数据，具体来讲是上述实施方式中的被加密的问候帧。另外，“第 2 访问密钥”例如是图 6 的访问密钥 b1，“访问密钥通知数据”例如是图 12 的加密访问密钥 D3。

[0307] 另外，在上述实施方式中，图 3 的接收部 8（更详细来讲是图 5 的帧分支处理部 21 和问候帧接收缓冲 22）作为访问密钥接收部而工作。

[0308] 另外，第 1 节点装置 1A 具有作为通过使用所生成的公用密钥对访问密钥通知数据进行解密来从访问密钥通知数据中取得第 2 访问密钥的访问密钥解密部而工作的组件。即，在上述实施方式中，图 3 的解密部 5（更详细来说是图 5 的问候帧解密部 25）作为上述访问密钥解密部而工作从而取得访问密钥 b1。

[0309] 另外，第 1 节点装置 1A 具有作为数据发送部而工作的组件。数据发送部向第 1 明文帧中附加使用公用密钥对包含根据第 1 明文帧计算出的第 1 散列值的数据进行加密得到的第 1 署名数据。并且，数据发送部使用解密得到的第 2 访问密钥对附加有第 1 署名数据的第 1 明文帧进行加密并作为第 1 加密帧发送。

[0310] 这里的“第 1 明文帧”的例子是包含关于图 15 所说明的由自组织 帧头 D9、明文 FID/D15 和明文帧体 D16 组成的明文净荷的明文帧。“第 1 散列值”的例子是根据还没有生成帧尾的明文帧（更准确来讲是根据明文净荷）计算出的图 15 的明文散列值 D17，“第 1 署名数据”的例子是加密署名 D21。根据实施方式不同，也可以还利用帧头计算散列值。另外，“第 2 访问密钥”具体来讲是图 6 的访问密钥 b1。

[0311] 在上述实施方式中，图 3 的加密部 4 和发送部 7（更详细来讲是图 5 的数据帧加密部 39、数据帧发送缓冲 43 和发送处理部 44）协同动作作为上述数据发送部而工作。

[0312] 另外，第 1 节点装置 1A 具有作为接收来自第 2 节点装置 1B 的第 2 加密帧的数据接收部而工作的图 3 的接收部 8（更详细来说是图 5 的帧分支处理部 21 和数据帧接收缓冲 24）。这里，所谓“第 2 加密帧”是利用第 1 访问密钥对第 2 明文帧进行加密得到的帧，“第 2 明文帧”是附加有利用上述公用密钥对包含第 2 散列值的数据进行加密得到的第 2 署名数据的帧。

[0313] 另外，第 1 节点装置 1A 具有作为数据解密部而工作的图 3 的解密部 5（更详细来说是图 5 的数据帧解密部 27）。上述数据解密部利用第 1 访问密钥对第 2 加密帧进行解密，并根据第 2 加密帧得到附加有第 2 署名数据的第 2 明文帧。

[0314] 在上述实施方式的说明中，结合从节点装置 1A 向节点装置 1B 发送数据帧的情况对图 15 的例子进行了说明，但是图 15 也适用于从节点装置 1B 向节点装置 1A 发送数据帧的情况。在这种情况下，图 15 的由自组织帧头 D9、净荷 D26 和帧尾 D27 组成的数据帧相当于从节点装置 1B 发送来的“第 2 加密帧”。

[0315] 并且，作为上述数据解密部而工作的节点装置 1A 的数据帧解密部 27 使用作为“第 1 访问密钥”的访问密钥 a1 得到第 2 明文帧。这里，“第 2 明文帧”包含由自组织帧头 D9、被解密的明文 FID/D28 以及被解密的明文帧体 D29 组成的明文净荷。另外，在“第 2 明文帧”中，由被解密的密文散列值 D30 和被解密的密文时刻 D31 组成的加密署名（相当于上述的“第 2 署名数据”）作为帧尾被附加。

[0316] 另外，第 1 节点装置 1A 具有作为一致性确认部而工作的组件。在上述实施方式中，图 5 的数据帧解密部 27 和确认部 29 协同动作作为一致性确认部而工作。具体来讲，作为一致性确认部的一部分的数据帧解密部 27 通过使用所生成的公用密钥对第 2 署名数据进行解密来取得第 2 散列值。并且，作为一致性确认部的一部分的确认部 29 根据第 2 明文帧计算第 3 散列值（例如图 15 的计算出的散列值 D32），并确认是否取得了第 2 散列值和上述第 3 散列值的一致性。

[0317] 另外，上述的数据发送部还可以使第 1 明文帧中包含用于唯一识别第 1 明文帧的第 1 识别符和表示第 1 发送时刻的信息。

[0318] 在上述实施方式中，数据帧生成部 40 也作为数据发送部的一部分而工作，数据帧生成部 40 使第 1 明文帧中包含作为“第 1 识别符”的图 17 的明文 FID/D15 和作为“表示第 1 发送时刻的信息”的明文时刻 D18。或者，数据帧生成部 40 也可以如图 15 那样使第 1 明文帧中包含加密时刻 D20，作为“表示第 1 发送时刻的信息”。明文时刻 D18 和加密时刻 D20 虽然有是明文或密文的区别，但是在“表示第 1 发送时刻”这一点上是相同的。

[0319] 另外，图 5 的接收数据帧处理部 30 还可以附加性地作为上述的一致性确认部而工作。也就是说，在从第 2 加密帧解密得到的第 2 明文帧中包含的第 2 识别符等于从过去接收过的第 3 加密帧解密得到的第 3 明文帧中包含的第 3 识别符的情况下，作为一致性确认部的接收数据帧处理部 30 也可以将第 2 和第 3 明文帧中的通过解密得到的信息表示较新的发送时刻的一方废弃。

[0320] 例如，若将图 17 的例子适用于从节点装置 1B 向节点装置 1A 发送的情况，则“第 2 明文帧”由自组织帧头 D9、明文净荷和作为明文帧尾的被解密的密文散列值 D46 组成。并且，明文净荷由被解密的明文 FID/D43、被解密的明文时刻 D44 以及被解密的明文帧体 D45 组成。另外，“第 2 识别符”相当于被解密的明文 FID/D43。

[0321] 并且，作为一致性确认部的接收数据帧处理部 30 如下面那样工作。即，接收数据帧处理部 30 在明文 FID/D43 等于过去接收过的其他的数据帧的 FID 的情况下，将通过解密得到的发送时刻（例如被解密的 明文时刻 D44）较新一方的数据帧废弃。

[0322] 这样，作为数据发送部以及一致性确认部的各部进行使用了识别符（具体来讲是 FID）的处理，由此节点装置 1A 能够检测出由非法的节点装置发送的帧。

[0323] 另外，网络内的多个节点装置（例如包含节点装置 1A 和 1B）的各自的公用密钥生成部 3，如上面所述那样每隔共同的时间、即第 2 时间就生成公用密钥。所以，多个节点装置的各自的时钟（例如图 5 的时钟 33）如果在即使无视也不会产生问题的程度的误差范围内互相同步，则在多个节点装置中生成公用密钥的定时也同步。

[0324] 但是，多个节点装置各自的时钟的时刻的错位也有可能随着时间扩大。所以，上述实施方式通过校正多个节点装置各自的时钟的时刻的错位在网络内的多个节点装置之间取得生成公用密钥的定时的同步。

[0325] 即，第 1 节点装置 1A 具有协同动作作为时刻同步帧发送部而工作的组件。时刻同步帧发送部生成包含表示第 1 节点装置 1A 中的第 1 当前时刻和在第 1 节点装置 1A 中进行了时刻校准的第 1 同步时刻的数据的第 1 时刻同步帧作为时刻同步帧并发送。

[0326] 例如，在图 19 的例子中，步骤 S703 以后的“第 1 同步时刻”是 12:00，在步骤 S706 中发送包含表示作为“第 1 当前时刻”的 13:40 的信息的时刻同步帧 P3。

[0327] 另外，虽然上述实施方式的时刻同步帧被利用时刻同步密钥加密，但是时刻同步帧没有被加密的实施方式也是可能的。所以，虽然在上述实施方式中图 5 的时刻同步部 9、时刻同步帧加密部 38、时刻同步帧发送缓冲 42 以及发送处理部 44 协同动作作为时刻同步帧发送部而工作，但是也可以省略时刻同步帧加密部 38。

[0328] 另外，第 1 节点装置 1A 具有作为从第 2 节点装置 1B 接收第 2 时刻同步帧的时刻同步帧接收部而工作的组件。这里，第 2 时刻同步帧包含表示第 2 节点装置 1B 中的第 2 当前时刻（例如在图 19 的例子中是 13:30）和在上述第 2 节点装置中进行了时刻校准的第 2 同步时刻（例如在图 19 的例子中是 10:00）的数据。

[0329] 在上述实施方式中，图 5 的帧分支处理部 21 以及时刻同步帧接收缓冲 23 协同动作作为上述时刻同步帧接收部而工作。

[0330] 并且，第 1 节点装置 1A 具有作为时刻更新部而工作的组件。时刻更新部比较根据第 2 时刻同步帧得到的第 2 同步时刻和第 1 节点装置 1A 存储的第 1 同步时刻。并且，如果第 2 同步时刻较新，则时刻更新部设定第 2 当前时刻作为第 1 节点装置 1A 中的当前时刻，来更新第 1 节点装置 1A 的时刻。

[0331] 具体来讲，图 5 的时刻同步部 9 作为时刻更新部而工作。另外，在上述实施方式中，由于时刻同步帧被加密，所以为了根据第 2 时刻同步帧得到第 2 同步时刻，时刻同步帧解密部 26 也作为时刻更新部的一部分而工作。

[0332] 并且，节点装置 1A 例如具有 DRAM15 作为存储部。该存储部将第 2 同步时刻作为通过作为时刻更新部的时刻同步部 9 更新第 1 节点装置 1A 的时刻进行了时刻校准的时刻进行存储。另外，图 3 以及图 5 的公用密钥生成部 3 根据作为时刻更新部的时刻同步部 9 进行了更新的时刻（具体来讲是图 5 的时钟 33 表示的时刻）对第 2 时间进行计时。

[0333] 根据上面大概描述的上述实施方式，在第 2 节点装置是合法的节点装置的情况下，第 2 节点装置保有和第 1 节点装置公用的公用密钥。所以，能够使用公用密钥安全地交换第 1 节点装置中生成的第 1 访问密钥和第 2 节点装置中生成的第 2 访问密钥。

[0334] 另外，第 1 节点装置能够使用通过解密得到的第 2 节点装置的第 2 访问密钥对数据加密并向第 2 节点装置发送。并且，第 1 节点装置还能够从第 2 节点装置接收使用第 1 节点自身生成的第 1 访问密钥加密后的数据。

[0335] 这样，根据上述实施方式，各节点装置自主地与其他的节点装置协同动作进行用于加密的动作。所以，即使在包含非常多的节点装置的网络中，也不会发生用于加密密钥的交换的流量集中的情况。

[0336] 另外，各节点装置为了自主地进行用于加密的动作，需要取得各节点装置根据时间生成并通过修改进行变更的公用密钥的变更定时的 同步。根据上述的实施方式，提供了构成简单并且不会增加网络负荷的、能够取得同步而自主地变更公用密钥的节点装置。

[0337] 另外，在上述的实施方式中，主要说明了节点装置，但是使计算机执行上述方法的

控制程序也包含在本发明的实施方式的一例中。该控制程序也可以通过由磁盘、光磁盘、非易失性的半导体存储器、光盘等的计算机能够读取的存储介质存储来提供，被加载到计算机上并由计算机执行。

[0338] 执行该控制程序的计算机内置在未图示的节点装置中或者与其连接，按照该控制程序控制上述未图示的节点装置以使上述未图示的节点装置和上述实施方式的节点装置 1 同样动作。例如，如果从其他的观点来看上述实施方式，也可以说成节点装置 1 的内置计算机、即 MPU11 按照闪存 16 中存储的控制程序控制节点装置 1 并使上述各处理在节点装置 1 中执行。

[0339] 另外，上述实施方式中示例的 RC4 是能够采用的加密算法的一个例子。也可以根据实施方式不同进行基于其他的加密算法的加密以及解密。例如，也可以使用流加密以外的加密算法。另外，分别使用了时刻同步密钥、公用密钥和访问密钥的加密以及解密也可以基于不同的加密算法。

[0340] 另外，问候帧、数据帧、时刻同步帧的格式当然不限定于上述实施方式中示例的格式。例如，各帧还可以包含上述实施方式中没有示例的字段。相反，如果帧是固定长度，帧大小 D8 的字段可以省略。

[0341] 并且，上述实施方式中示例的“10 分钟”等的具体的数值只不过是为了帮助理解才表示的，可以根据实施方式设定各种各样的具体的数值。

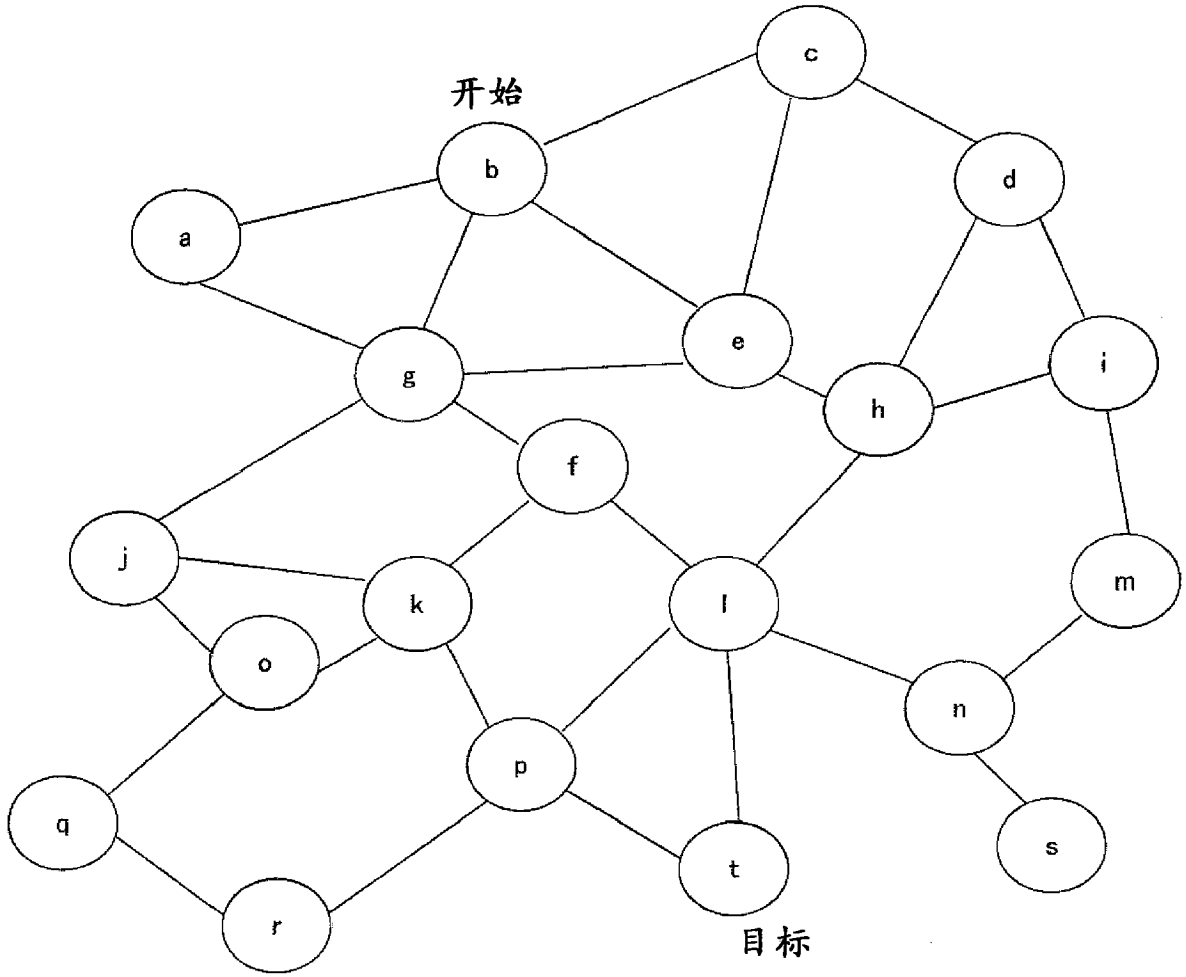


图 1

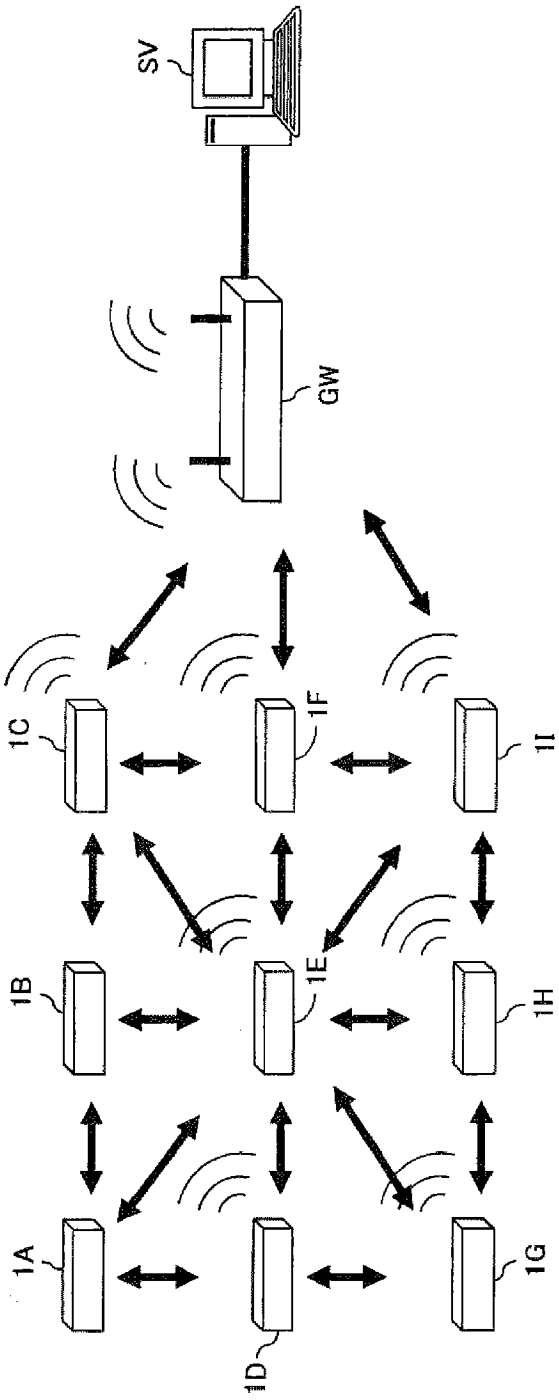


图 2

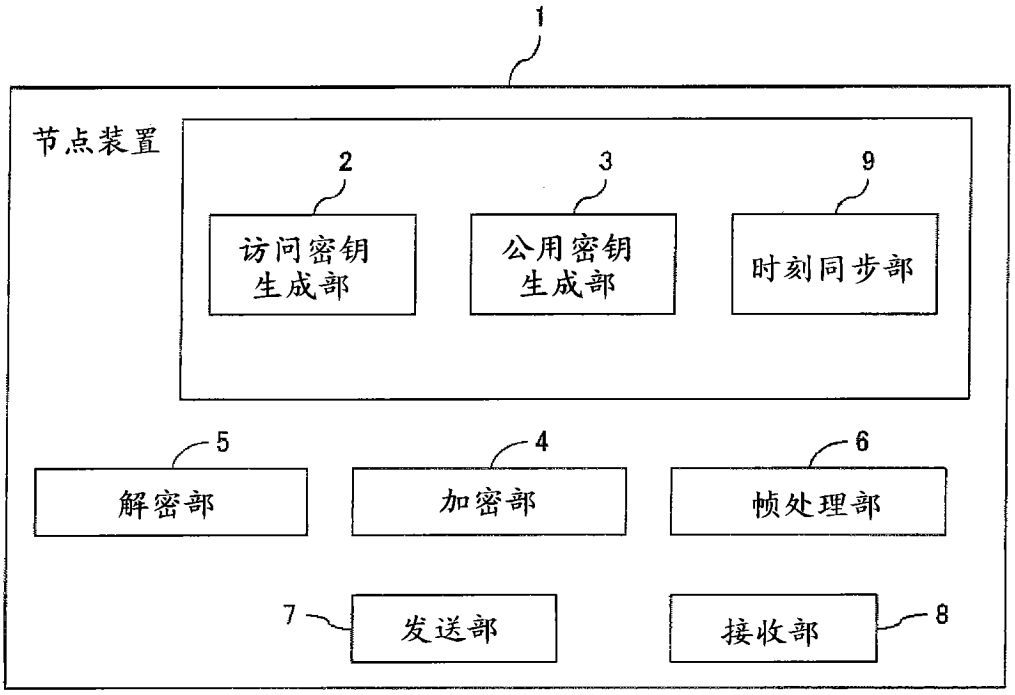

1
节点装置
2
访问密钥生成部
3
公用密钥生成部
9
时刻同步部
5
解密部
4
加密部
6
帧处理部
7
发送部
接收部
8

图 3

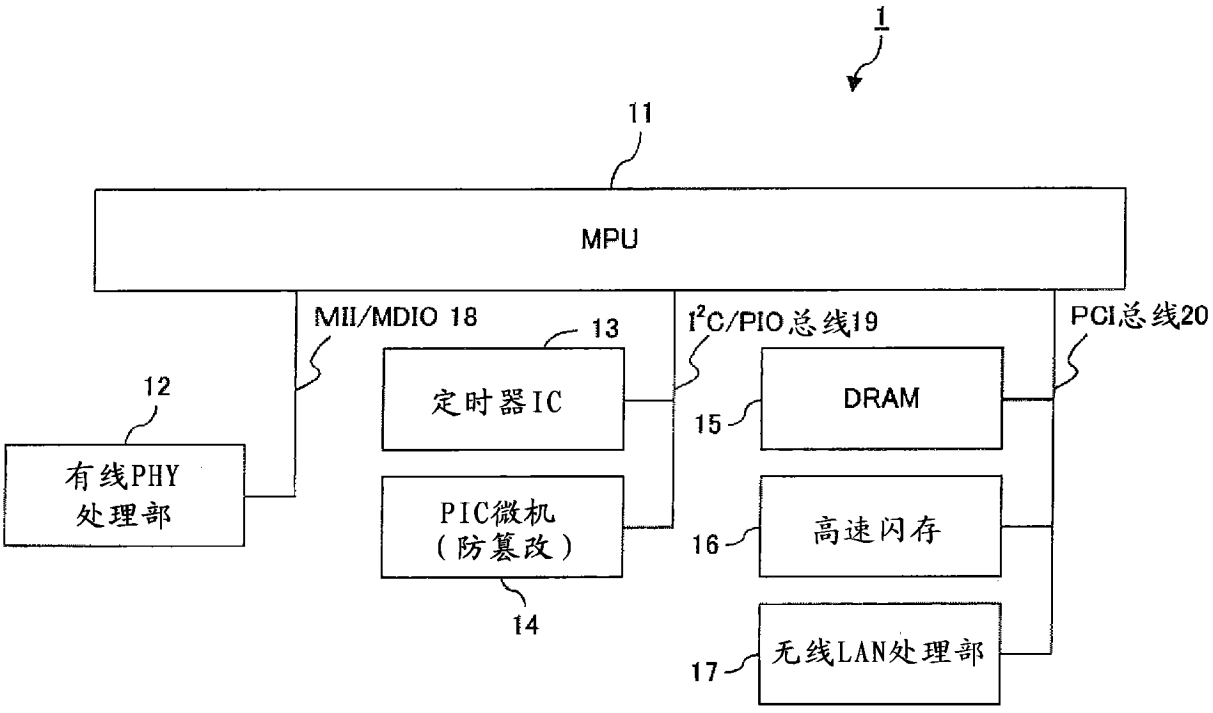

1
11
MPU
MII/MDIO 18
I²C/PIO总线19
PCI总线20
13
定时器IC
12
有线PHY处理部
15
DRAM
PIC微机（防篡改）
16
高速闪存
14
17
无线LAN处理部

图 4

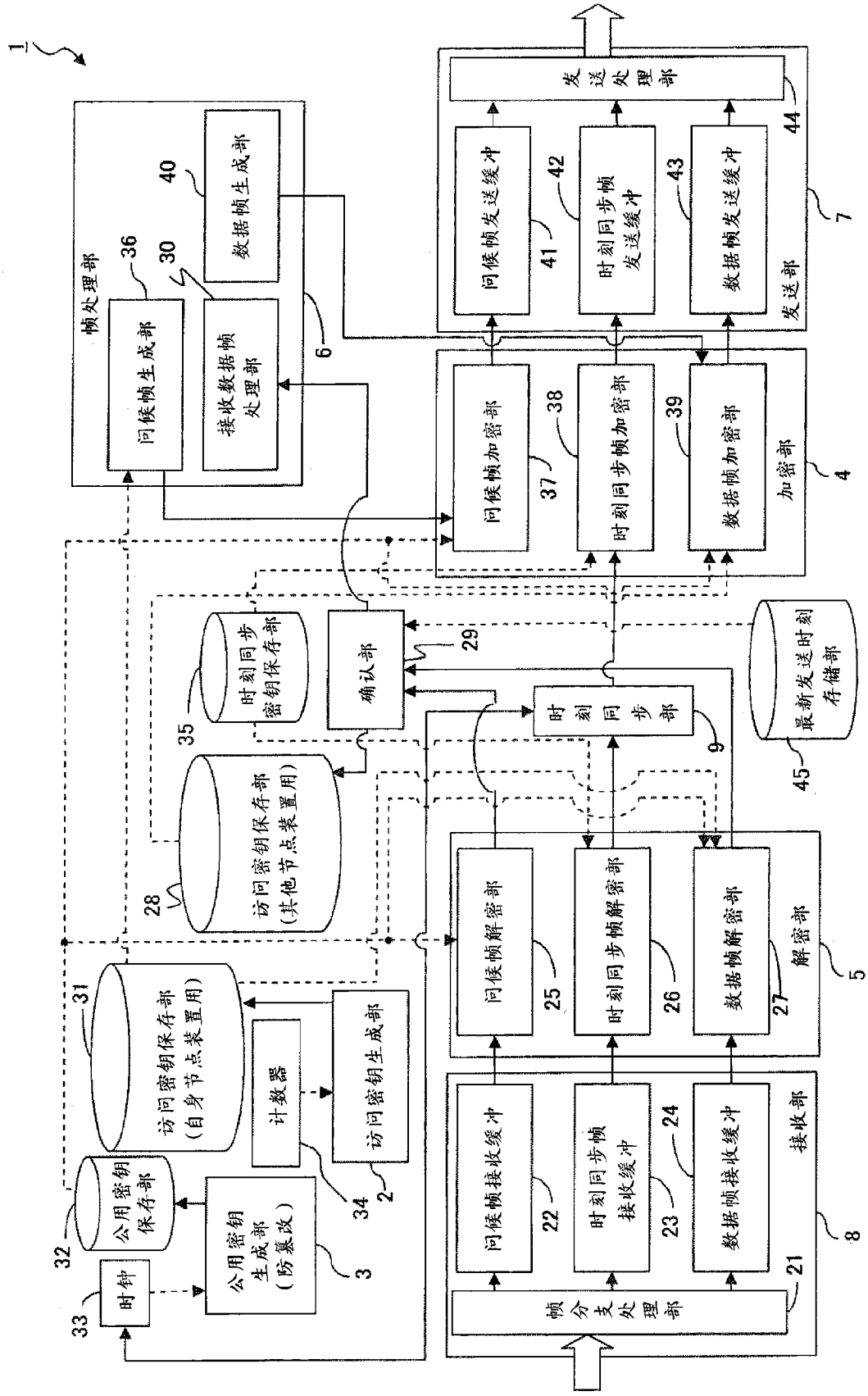

1
帧处理部
问候帧生成部
接收数据帧处理部
数据帧生成部
36
30
40
6
发送处理部
问候帧发送缓冲
时刻同步帧发送缓冲
数据帧发送缓冲
41
42
43
44
发送部
7
问候帧加密部
时刻同步帧加密部
数据帧加密部
37
38
39
加密部
4
时刻同步密钥保存部
确认部
29
35
时刻同步部
9
最新发送时刻存储部
45
访问密钥保存部（其他节点装置用）
28
问候帧解密部
时刻同步帧解密部
数据帧解密部
25
26
27
解密部
5
访问密钥保存部（自身节点装置用）
31
计数器
访问密钥生成部
2
34
问候帧接收缓冲
时刻同步帧接收缓冲
数据帧接收缓冲
22
23
24
接收部
8
公用密钥保存部
32
公用密钥生成部（防篡改）
3
时钟
33
帧分支处理部
21

图 5

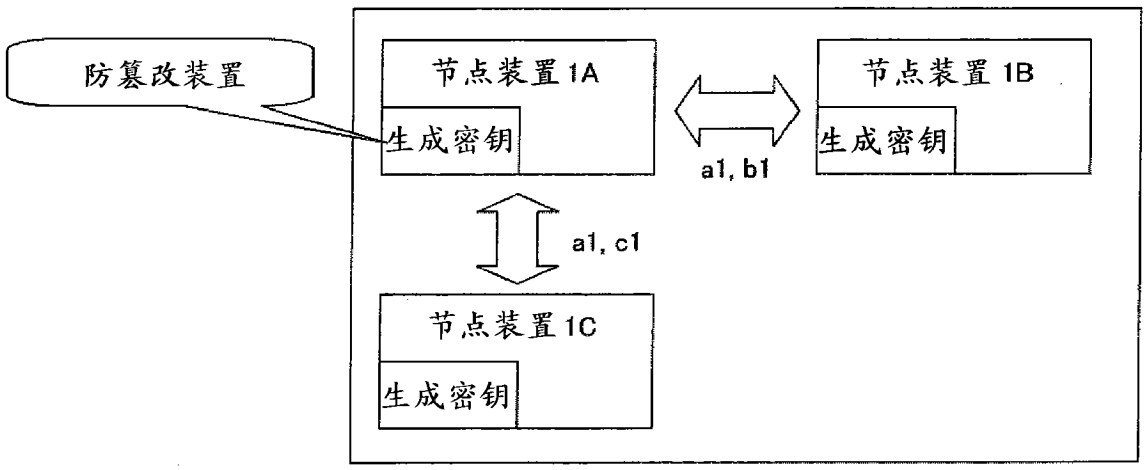


图 6

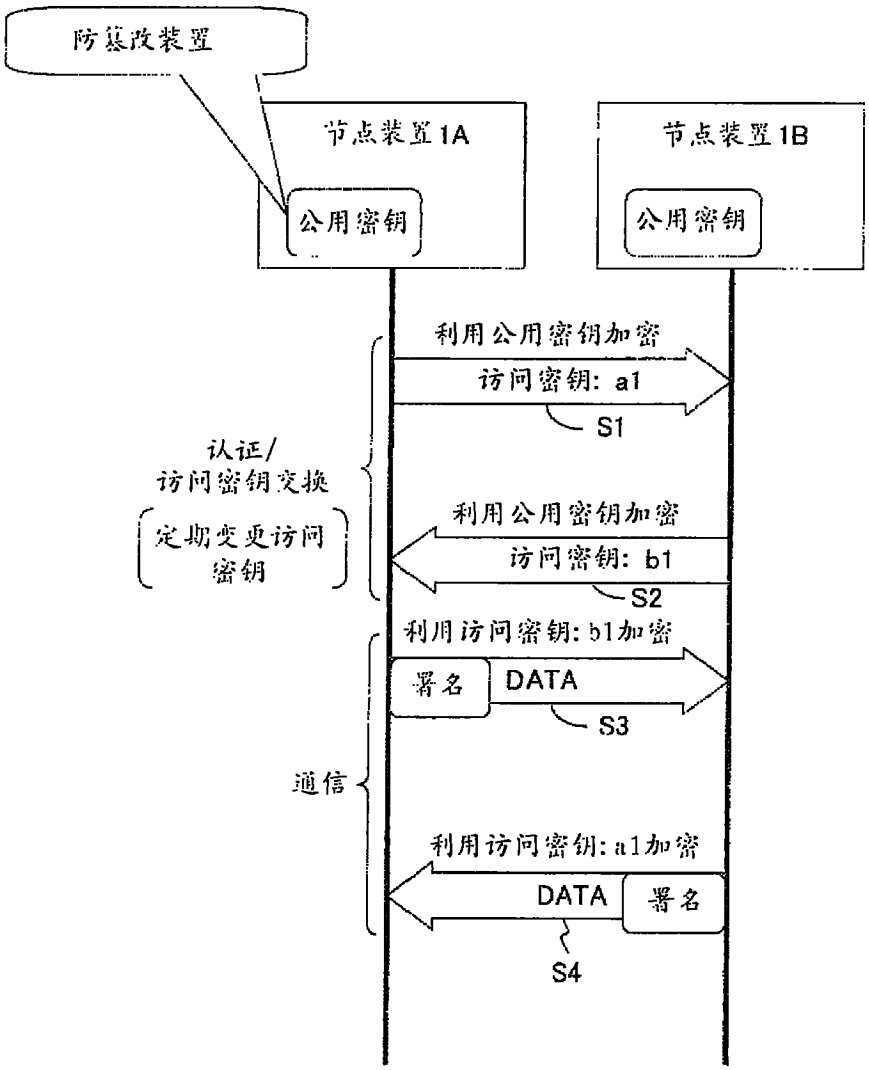


图 7

帧				署名
帧头	FID	时刻	帧体	Kt(散列(帧))

图 8

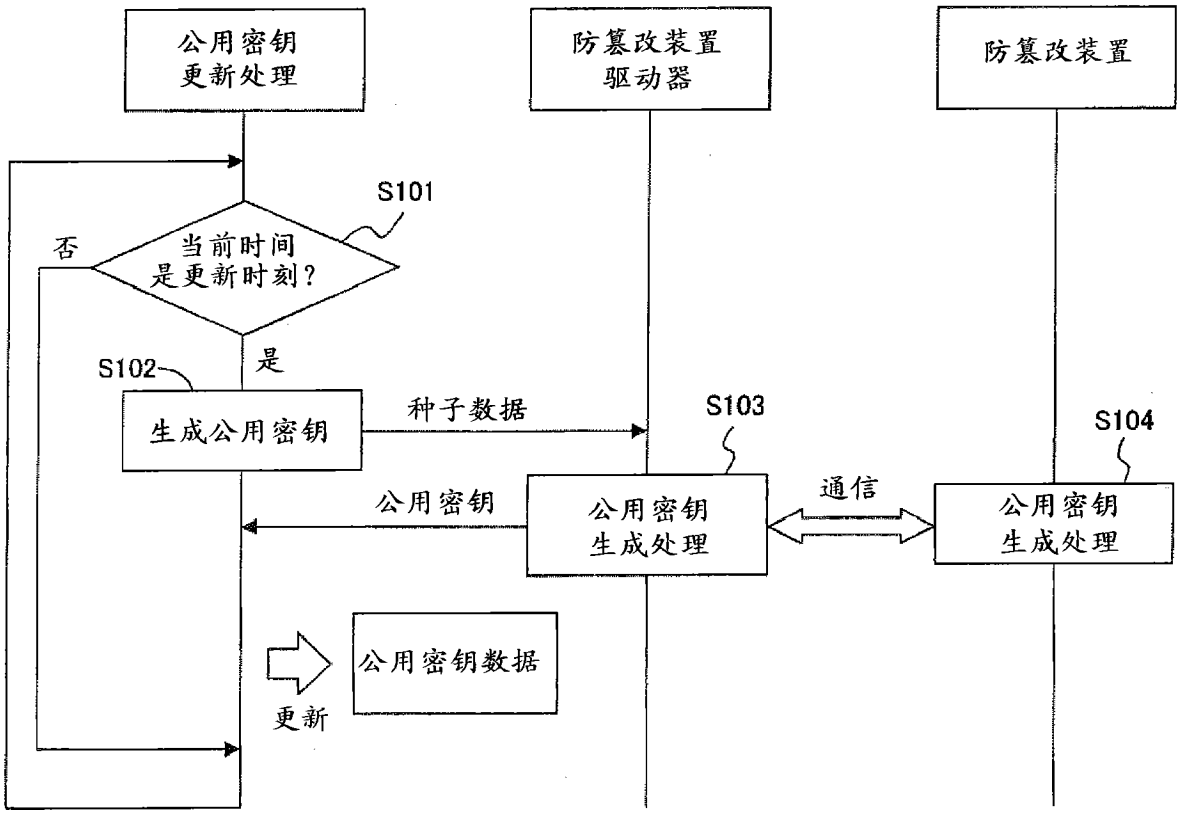

公用密钥
更新处理
防篡改装置
驱动器
防篡改装置
S101
当前时间
是更新时刻?
否
是
S102
生成公用密钥
种子数据
S103
S104
公用密钥
公用密钥
生成处理
通信
公用密钥
生成处理
公用密钥数据
更新

图 9

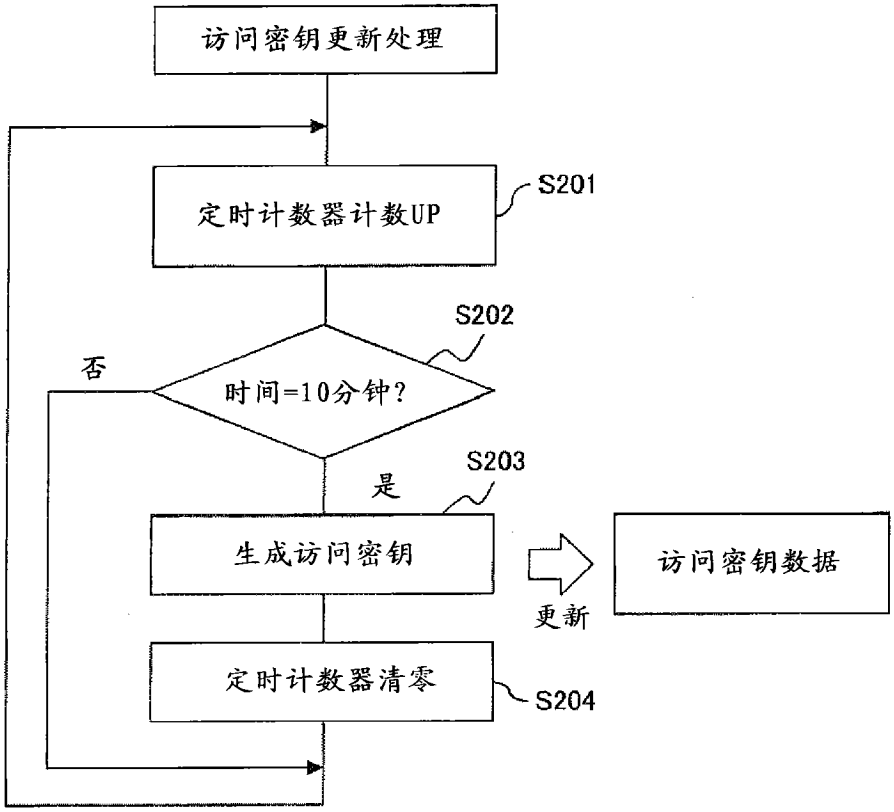

访问密钥更新处理
定时计数器计数UP
S201
S202
否
时间=10分钟?
S203
是
生成访问密钥
访问密钥数据
更新
定时计数器清零
S204

图 10

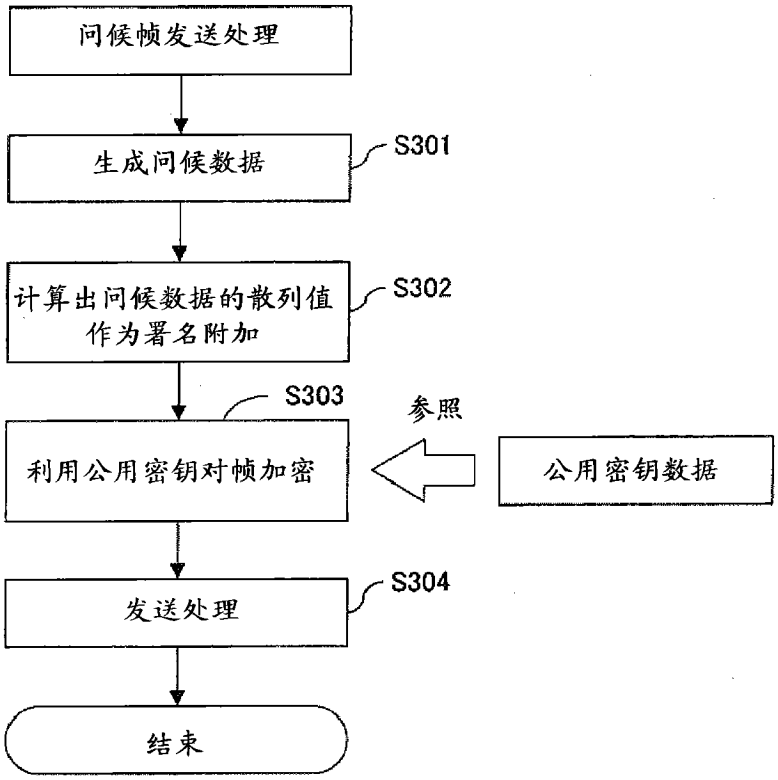

问候帧发送处理
生成问候数据
S301
计算出问候数据的散列值
作为署名附加
S302
S303
参照
利用公用密钥对帧加密
公用密钥数据
发送处理
S304
结束

图 11

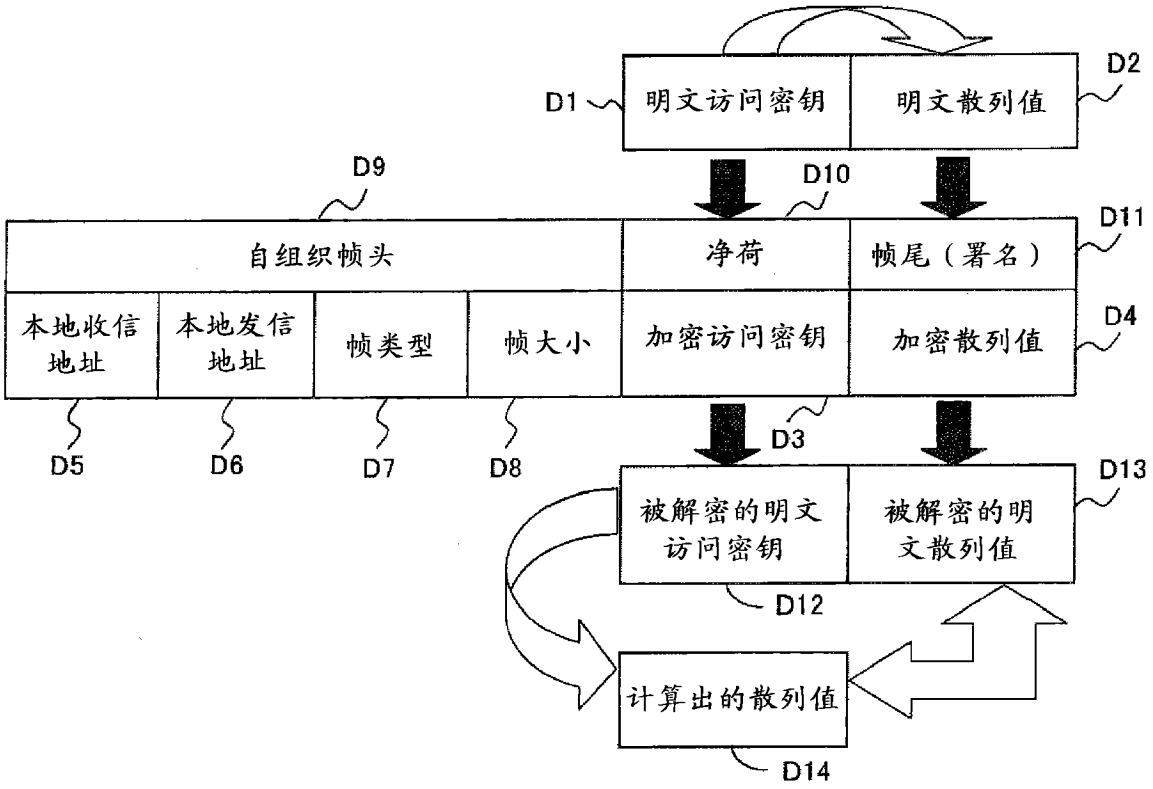

D1
明文访问密钥
明文散列值
D2
D9
D10
D11
自组织帧头
净荷
帧尾（署名）
本地收信地址
本地发信地址
帧类型
帧大小
加密访问密钥
加密散列值
D4
D5
D6
D7
D8
D3
D13
被解密的明文访问密钥
被解密的明文散列值
D12
计算出的散列值
D14

图 12

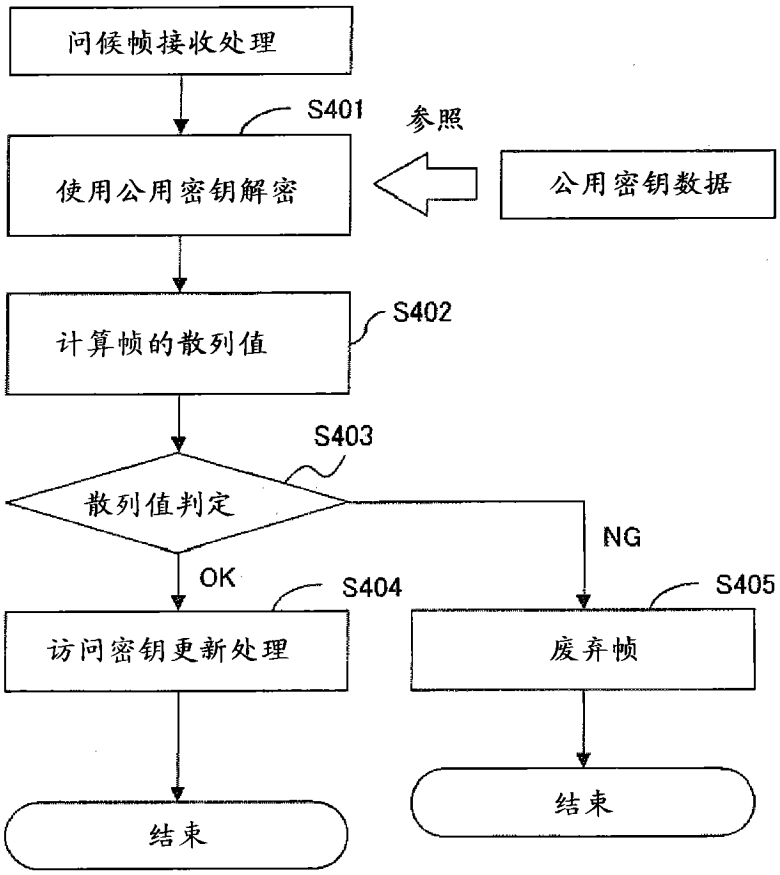

问候帧接收处理
S401
参照
使用公用密钥解密
公用密钥数据
计算帧的散列值
S402
S403
散列值判定
NG
OK
S404
S405
访问密钥更新处理
废弃帧
结束
结束

图 13

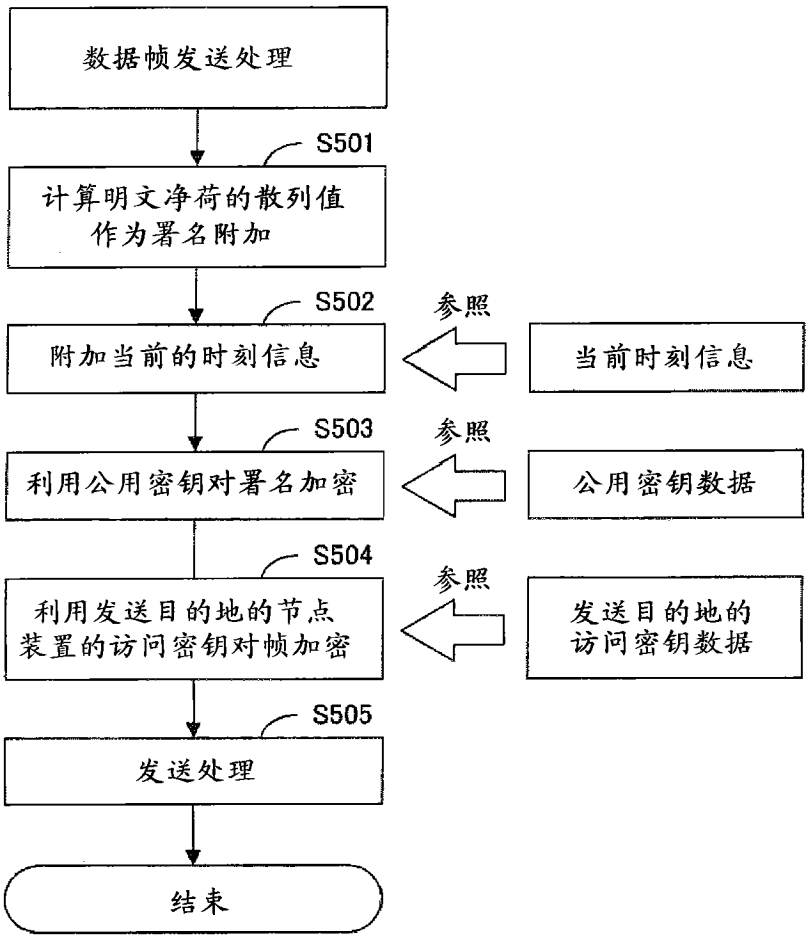

数据帧发送处理
S501
计算明文净荷的散列值
作为署名附加
S502
附加当前的时刻信息
参照
当前时刻信息
S503
利用公用密钥对署名加密
参照
公用密钥数据
S504
利用发送目的地的节点
装置的访问密钥对帧加密
参照
发送目的地的
访问密钥数据
S505
发送处理
结束

图 14

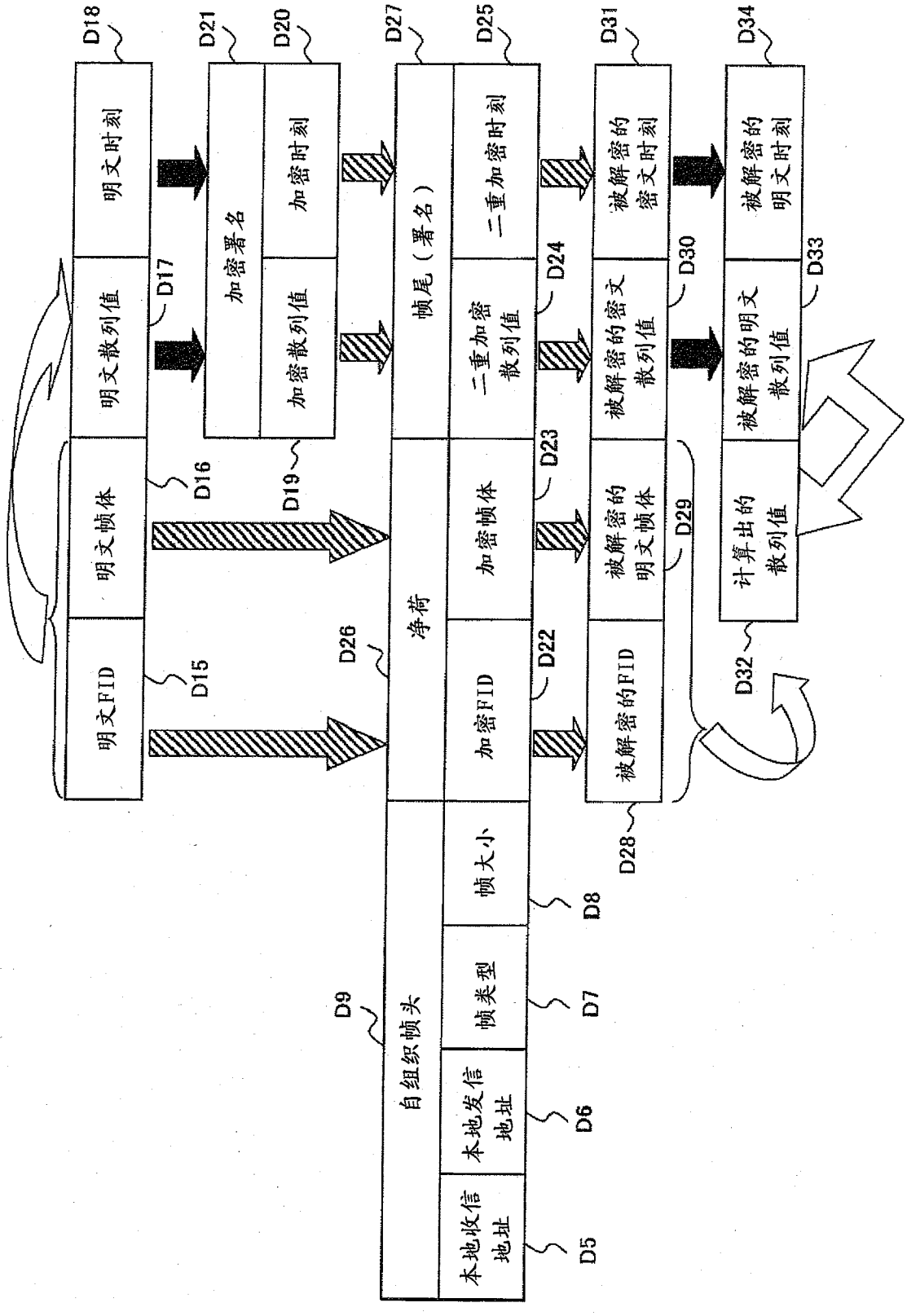

D18
明文时刻
D21
D20
D27
D25
D31
D34
明文散列值
D17
加密署名
加密时刻
帧尾（署名）
二重加密时刻
被解密的密文时刻
被解密的明文时刻
明文帧体
D16
D19
D24
D30
D33
加密散列值
二重加密散列值
被解密的密文散列值
被解密的明文散列值
明文FID
D15
D26
D23
D29
净荷
加密帧体
被解密的明文帧体
计算出的散列值
D22
D32
加密FID
被解密的FID
帧大小
D8
D28
自组织帧头
帧类型
D7
本地发信地址
D6
本地收信地址
D5
D9

图 15

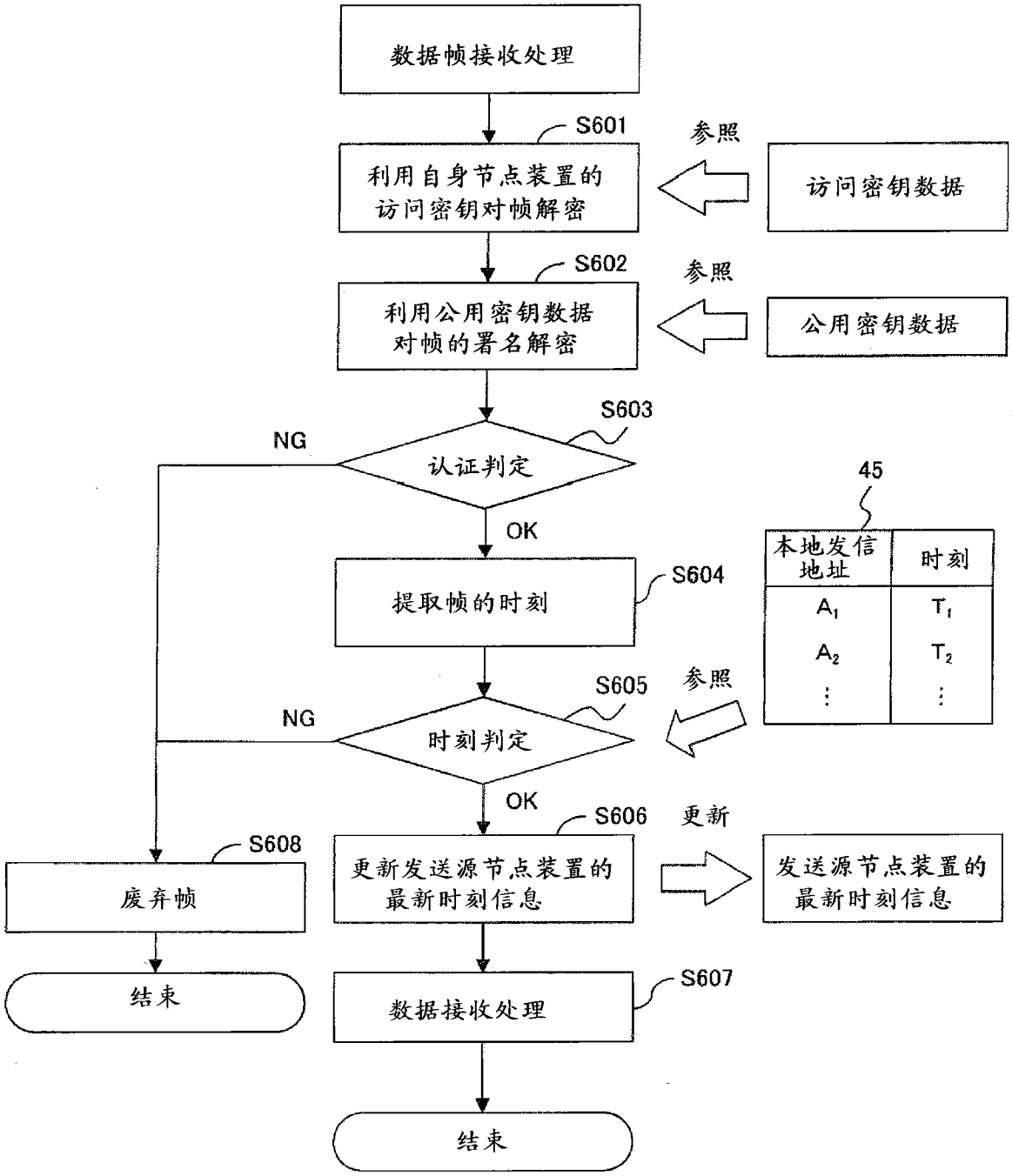

数据帧接收处理
S601
利用自身节点装置的访问密钥对帧解密
参照
访问密钥数据
S602
利用公用密钥数据对帧的署名解密
参照
公用密钥数据
S603
认证判定
NG
OK
45
本地发信地址
时刻
A1
T1
A2
T2
S604
提取帧的时刻
S605
时刻判定
参照
NG
OK
S606
更新
更新发送源节点装置的最新时刻信息
发送源节点装置的最新时刻信息
S608
废弃帧
结束
S607
数据接收处理
结束

图 16

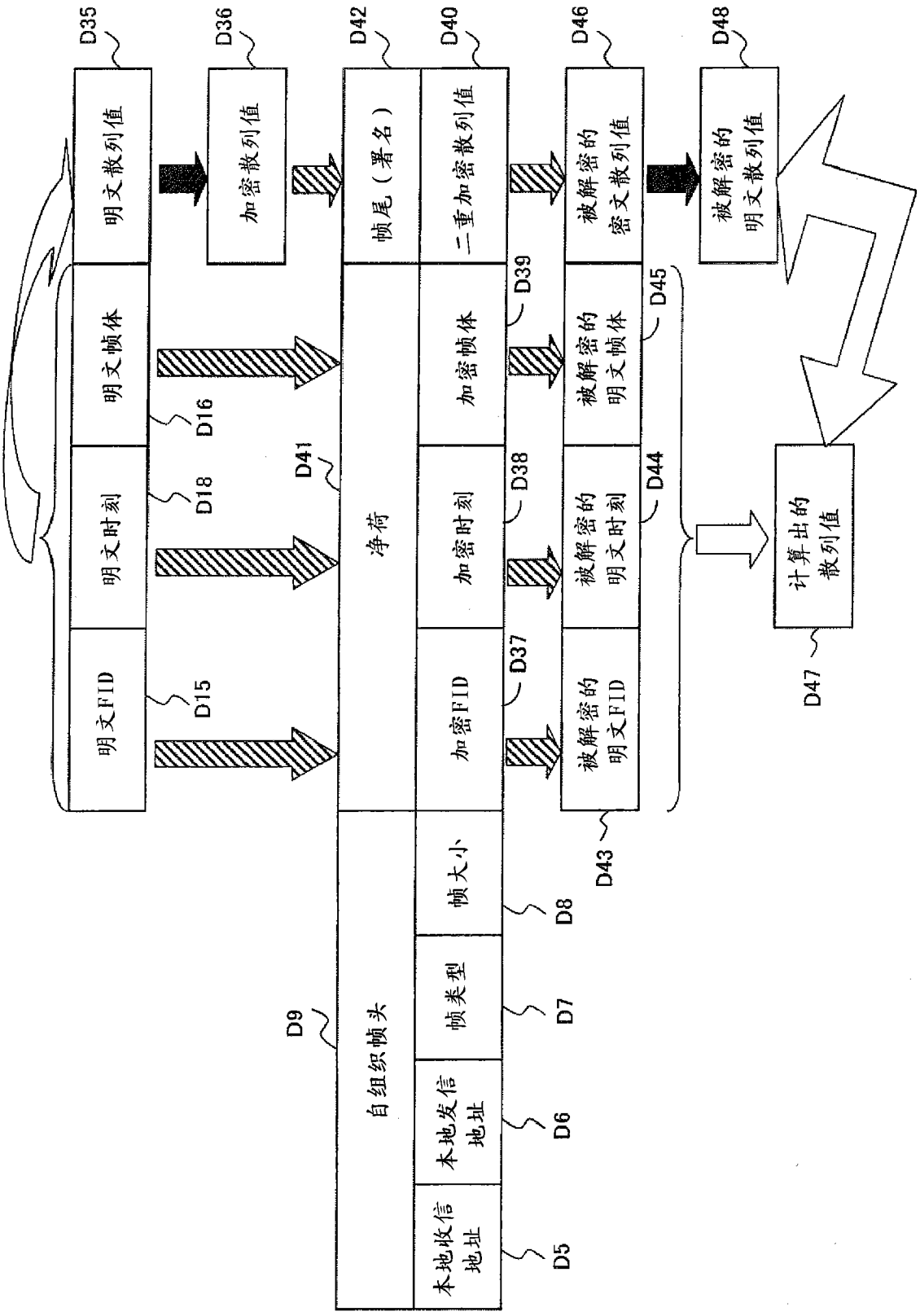

D35
明文散列值
D36
加密散列值
D42
帧尾（署名）
D40
二重加密散列值
D46
被解密的密文散列值
D48
被解密的明文散列值
明文帧体
明文时刻
明文FID
D16
D18
D15
D41
净荷
加密帧体
加密时刻
加密FID
D39
D38
D37
D45
D44
被解密的明文帧体
被解密的明文时刻
被解密的明文FID
D43
计算出的散列值
D47
自组织帧头
帧大小
帧类型
本地发信地址
本地收信地址
D9
D8
D7
D6
D5

图 17

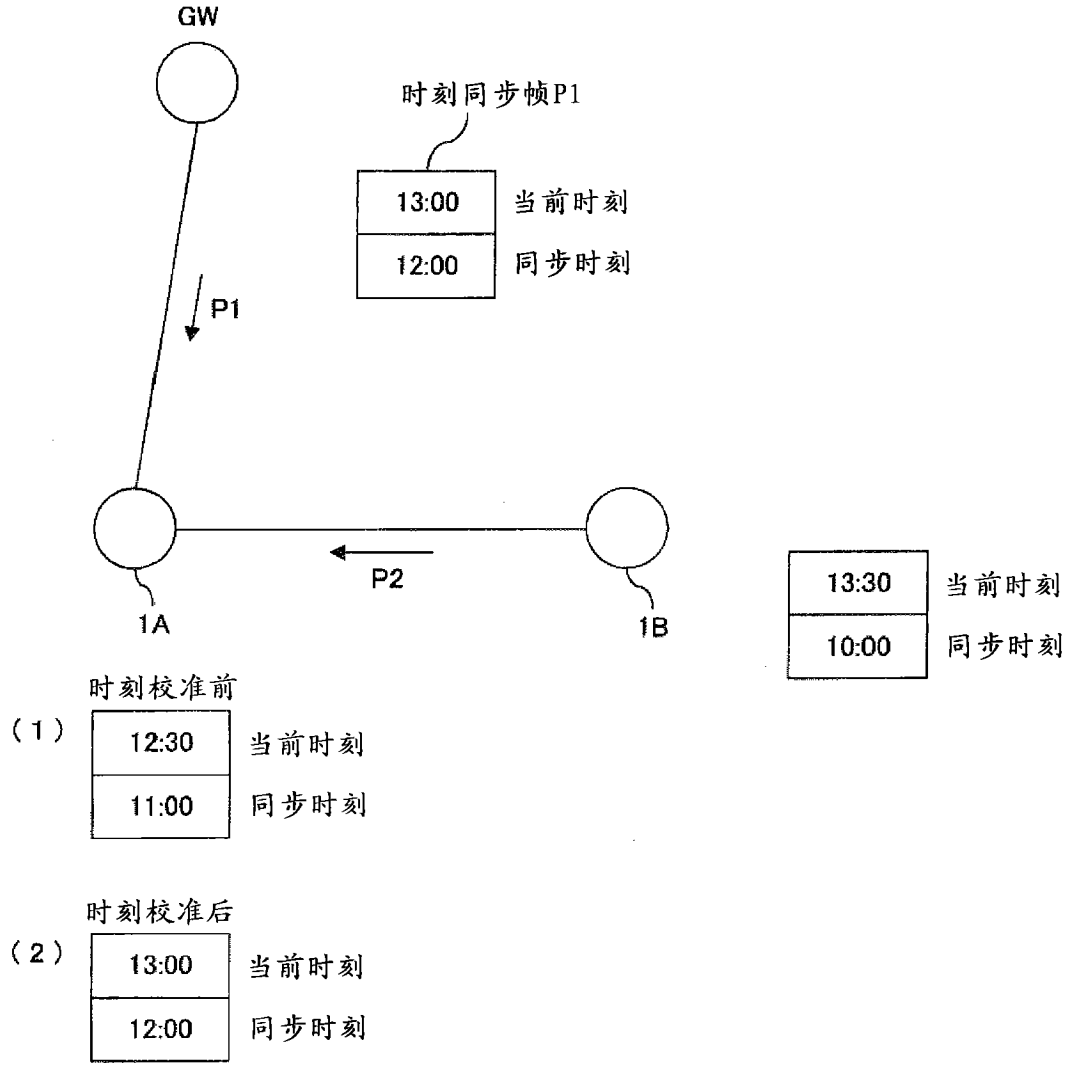

GW
时刻同步帧P1
13:00
当前时刻
12:00
同步时刻
P1
P2
1A
1B
13:30
当前时刻
10:00
同步时刻
时刻校准前
（1）
12:30
当前时刻
11:00
同步时刻
时刻校准后
（2）
13:00
当前时刻
12:00
同步时刻

图 18

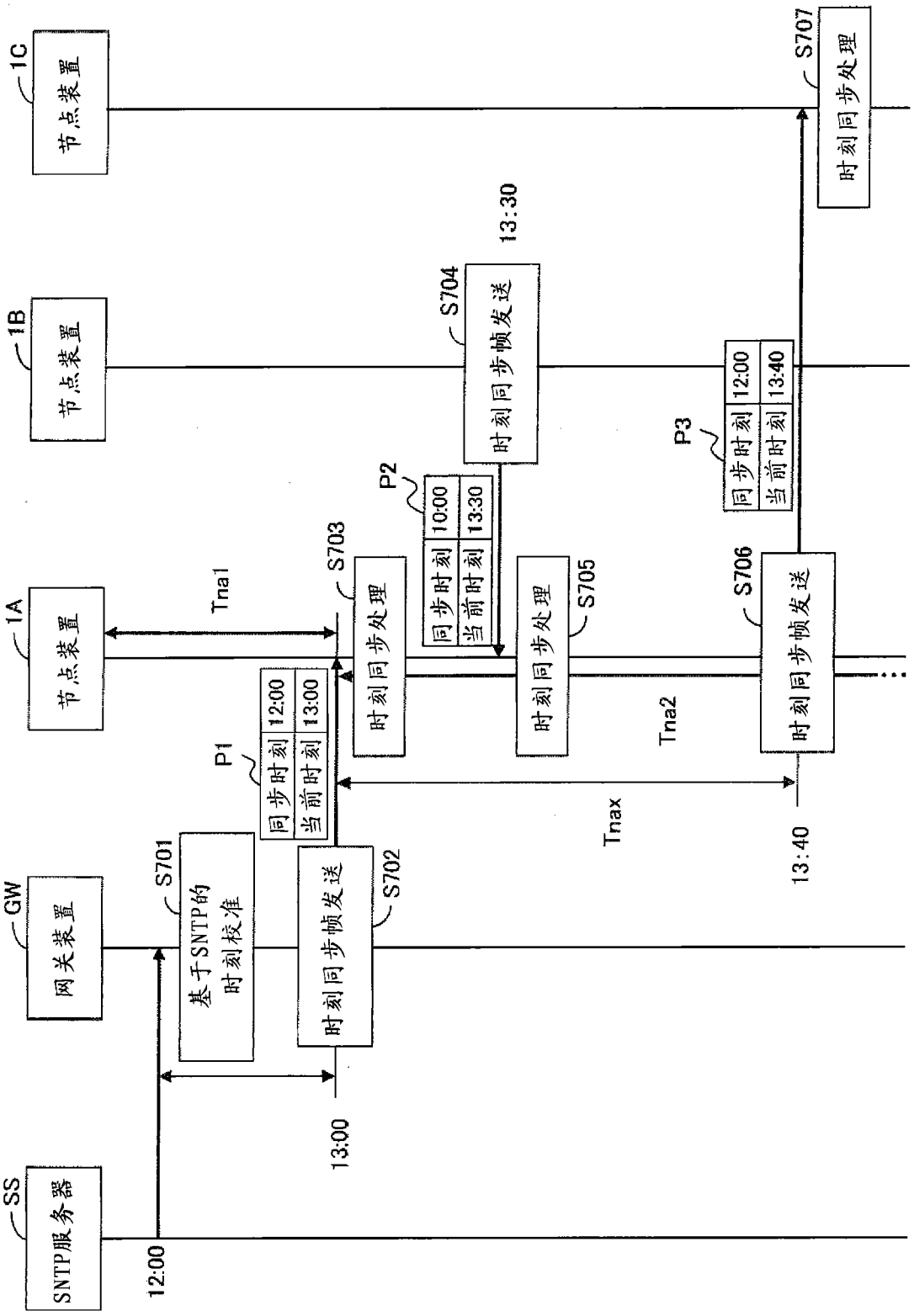

SS
SNTP服务器
GW
网关装置
1A
节点装置
1B
节点装置
1C
节点装置
12:00
13:00
13:40
基于SNTP的时刻校准
S701
时刻同步帧发送
S702
时刻同步处理
S703
时刻同步帧发送
S704
13:30
时刻同步处理
S705
时刻同步帧发送
S706
时刻同步处理
S707
Tna1
Tna2
Tnax
P1
同步时刻 12:00
当前时刻 13:00
P2
同步时刻 10:00
当前时刻 13:30
P3
同步时刻 12:00
当前时刻 13:40

图 19

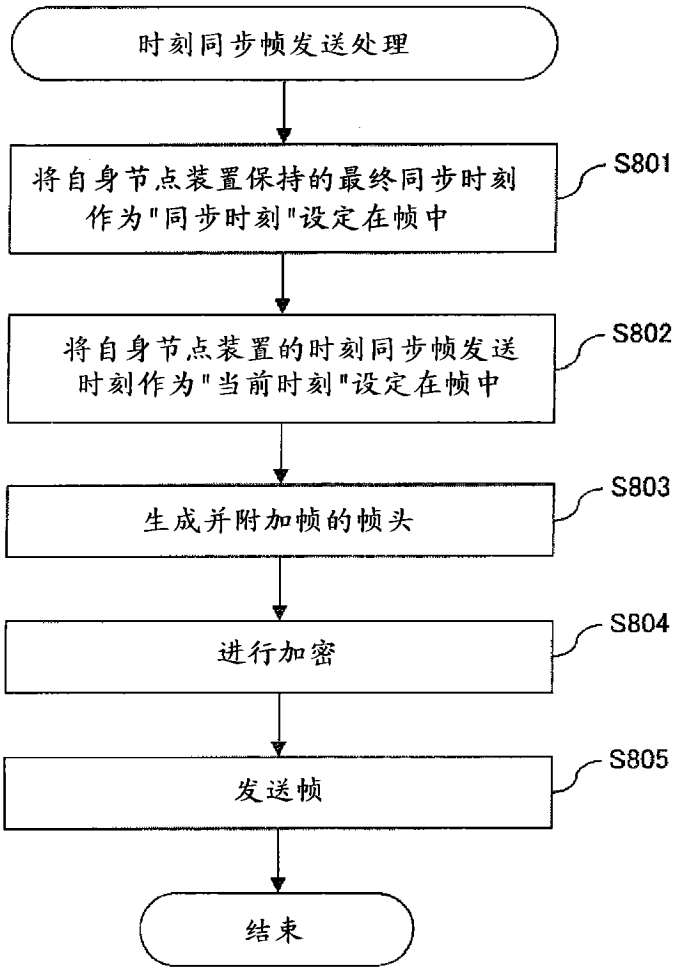

时刻同步帧发送处理
将自身节点装置保持的最终同步时刻作为"同步时刻"设定在帧中
S801
将自身节点装置的时刻同步帧发送时刻作为"当前时刻"设定在帧中
S802
生成并附加帧的帧头
S803
进行加密
S804
发送帧
S805
结束

图 20

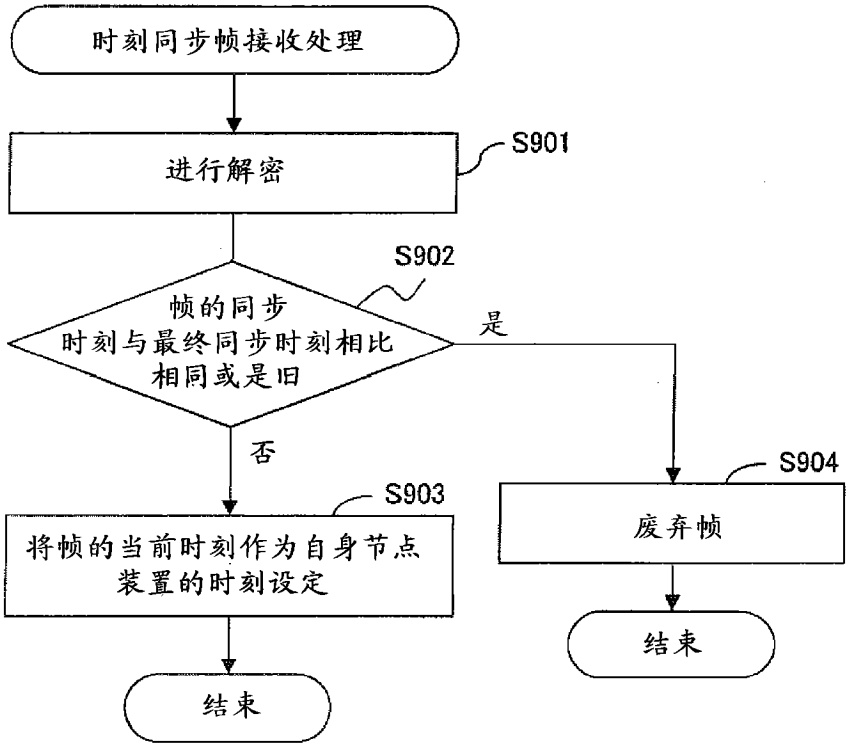

时刻同步帧接收处理
进行解密
S901
S902
帧的同步
时刻与最终同步时刻相比
相同或是旧
是
否
S903
将帧的当前时刻作为自身节点
装置的时刻设定
结束
S904
废弃帧
结束

图 21